Protecting Management Information Systems: Virtual Private Network Competitive Advantage

SID SIRISUKHA
A.A.S. (Morris, USA), B.S. (Caldwell, USA), M.S. (Stevens Tech, USA)

a thesis submitted to the graduate faculty of design and creative technologies
AUT University
in partial fulfilment of the
requirements for the degree of
doctor of philosophy

School of Computing and Mathematical Sciences

Auckland, New Zealand
2007

Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the qualification of any other degree or diploma of a University or other institution of higher learning, except where due acknowledgement is made in the acknowledgements.

.....

Signature

Acknowledgements

This thesis was completed at the Faculty of Design and Creative Technologies of the AUT University in the New Zealand. While conducting this research project I received support from many people in one way or another, without whose support, this thesis would not have been completed in its present form. It is my pleasure to take this opportunity to thank all of you, without the intention or possibility to be complete. I would like to apologize to those I do not mention by name here; however, I highly valued your kind support.

First, I would like to deeply thank my supervisors, Dr. Brian Cusack and Prof. Albert Yeap. Dr. Cusack provided me with the freedom to explore research directions and choose the routes that I wanted to investigate. Dr. Cusack, I would like to thank you very much for your daily supervision. I enjoyed our discussions and have learned a great deal from you. I also would like to thank Prof. Albert Yeap, who has kindly agreed to be my secondary supervisor. Prof. Yeap has taught me many valuable lessons during the early years of my Ph.D. study. I strongly believe that what I have learned during the PhD study period will be infinitely profitable for the rest of my life. For this I am eternally grateful. Thank you, from deep in my heart!

I would like to acknowledge the friendship and mentorship of my fellow Ph.D. students Stephen Thorpe, Janette Hamilton-Pearce, and Dilip Limbu for your support. I would like to deeply thank Mikhail Kotykhov for your kind assistance over the past several years. Without your help, my life would have been more difficult. I would like to thank all of you.

I would like to express my deep appreciation to James McGurick, who helped a great deal in my collection of data in USA. I would like to thank you to Anan Sangsoi, Ludarat Nitipoj, and Pramjit Tunpich, my former colleagues in Bangkok, Thailand, for their encouragement, and support during my data collecting in Thailand.

I am especially indebted to my former postgraduate supervisors, Professors Jerry Luftman, and Dr. Ira Sack at Stevens Institute of Technology New Jersey, USA for leading me to the IS world.

I wish to express my sincere thanks to my father, Kittidej Sirisukha, and my mother, Somsuk Sirisukha, who continual support, encouragement, love, praying for my progress and for teaching me the values in life that brought me where I am today. I greatly appreciate my wife, Supahwadee Sirisukha for fulfilling take care of our daughter, Janny who is 8 year-old,

and son, Prom Jack who is 4 year-old, during my Ph.D. study. I greatly appreciate my two sisters for fulfilling my duty to take care of our parents while I pursued Ph.D. degree.

Abstract

Information security technologists and business scholars are motivated by a desire to understand how and to what extent the application of IT within enterprise systems leads to improved and secured organizational performance. An effective relationship between business and IT professionals is a primary determinant of success in gaining business advantage through the enterprise system. As business innovation has relied increasingly on partnerships between business and IT professional, a different perspective of how IT professionals view their organizational contributions was needed for organizations to remain competitive. Business knowledge is essential if IT professionals are to create linkages with other organizational units and have a wider perspective about business objectives, thus achieving fit between IT and organizational strategies. Organizations have started responding to this challenge by demanding more business acumen in their IT staff. The focus of this study is on the knowledge that is beyond that of independent business and IT only domain knowledge of information security. Therefore, technical areas of knowledge, such as hardware and software, all of which are closely associated with IT skills, are not discussed in this thesis. This is not to declare that such knowledge is not important. Clearly technical knowledge is part of the IT professional's overall information security technology expertise, but this study is about the organization proficiency of business and the IT professional, and is therefore interested in what enables business and IT professionals to apply their business domain and technical knowledge in ways that are beneficial to the organization and to act cooperatively with their customers and business partners.

The purpose of this study is to employ the triangulation method to identify the theoretical links and empirically examine the association between business and IT perspective of information security. An important contribution of this study is the identification of business and IT perspectives on information security technology. By establishing the link between business and IT, the study focuses and evaluates Virtual Private Network (VPN) as an information security technology to find out if VPN can secure and gain competitive advantage by partisan business process and organization performance. This study articulates distinctive characteristics of Virtual Private Network and management processes that extend the range of applicability across diverse business segments. It distinguishes between business and IT and explains why the exploitation of a complementary set of related information security entities (such as VPN) across multiple functions create competitive

advantages even across a diverse set of businesses that have limited opportunity to exploit business process and organization performance.

The most important direct predictor of this study is a high level of communication between business and IT. However, one cannot mandate meaningful communication between individuals. IT people have to earn the right to play a meaningful role in management forums. Based on the findings from this study, one important way for an IT person to be heard is for him/her to devote the time necessary to create competitive advantage and develop shared domain knowledge, the most influential construct in the research model. An IT person needs to understand the leverage points of the industry, the history and current issues of the business units, and to learn to apply business oriented objectives in the application of technology to business problems. This change in view would help focus their attention on security technology and ideas that could produce the most benefit and create competitive advantage, rather than those that offer the most technical promise.

Table of Contents

Chapter – 1 Introduction

Chapter – 2 The IT Context

Chapter – 3 The Business IT Context

Chapter - 4 Research Methodology

Chapter – 5 Research Findings

Chapter – 6 Discussion of Findings

Chapter – 7 Recommendations

Appendix

List of Tables

List of Figures

List of Abbreviations

AH	Authentication Header
AHP	Analytic Hierarchy Process
ARP	Address Resolution Protocol
ARPANET	Advanced Research Projects Agency Network
ASCII	American Standard Code for Information Interchange
BIS	Business Information System
CBT	Core Based Tree
CCITT	Consultative Committee for International Telephone & Telegraphy
CEO	Chief executive officer
CFO	Chief Financial Officer
CIFS	Common Internet File System
CIO	Chief Information officer
COBIT	Control Objectives for Information and related Technology
COSO	Committee of Sponsoring Organization
DES	Data Encryption Standard
DMZ	Demilitarized Zone
DNS	Domain Name System
DVMRP	Distance Vector Multicast Routing Protocol
EDI	Electronic Data Interchange
EIS	Expert Information Systems
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HTML	Hypertext Markup Language
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICV	Integrity Check Value
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IPng	Internet Protocol next generation
IPSec	IP Security
IPv4	Internet Protocol Version 4

IPv6	Internet Protocol Version 6
IS	Information Systems
ISACA	Information Systems Audit and Control Association
ISAKMP	Internet Security Association and Key Management Protocol
ISO	International Standards Organization
ISP	Internet Service Provider
IT	Information Technology
ITIL	Information Technology Information Library
L2TP	Layer Two Tunnelling Protocol
LAN	Local Area Network
LSA	Lotus Solution Architecture
MAC	Media Access Control
MBO	Management by Objective
MD5	Message Digest 5
MIS	Management Information System
MOSPE	Multicast Open Shortest Path First
NAS	Network Access Server
NIST	National Institute of Standards and Technology
OSI	Open Systems Interconnection
PIM-DM	Protocol Independent Multicast - Dense Mode
PIM-SM	Protocol Independent Multicast - Sparse Mode
PoP	Point Of Presence
POS	Point of Sale
PPTP	Point-to-Point Tunnelling Protocol
QoS	Quality of Service
RADB	Reunion Address DataBase
RAS	Remote Access Server
RPC	Remote Procedure Calls
SAM	Strategic Alignment Model
SAS	Statement on Auditing Standard
SDLC	System Development Life Cycle
SG	Security Gateway
SISP	Strategic Information Systems Planning
SMTP	Simple Mail Transfer Protocol

SP	Special Publication
SPI	Security Parameter Index
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TTL	Time to Live
UDP	User Datagram Protocol
VPN	Virtual Private Network
WAN	Wide area network

CHAPTER 1

INTRODUCTION

1.0 BACKGROUND

This research explores information security systems in the context of effective organisational controls. A distinguishing characteristic of the organisational control of information systems security in the business context is the conflict between business and IT objective setting and the subsequent levels of risk for the enterprise. Inadequate resolution of this issue implicates business managers in a volatility that has serious consequences for business competitive advantage and the compromise of business assets. The purpose of this study is to employ the triangulation method to develop the theoretical links and empirically examine the association between the business and IT perspective of information security. An important contribution of this study is the identification of business and IT perspectives on information security technology. By examining the linkages between business and IT, this study focuses and evaluates Virtual Private Network (VPN) as an information security technology to find out if VPN can secure and gain competitive advantage by partisan business process and organization performance.

The effective relationship between business and IT is a primary determinant of success in gaining business advantage through IT (Gelinas, Sutton, & Fedorowicz, 2004). Consequently, business innovation relies even more strongly on partnerships between IT and business people, and a different perspective of how IT professionals view their organizational contributions is needed for organizations to regain competitive advantages. For example, Fichman (2001) points out that IT people focus on information systems in organizations, and concludes that IT people understand how organizational phenomena affect the development and use of technologies and how technologies shape organizations that are central to the field's agenda, but tend to prefer IT centric interpretations of the business organisation. According to West (2001), business people tend to pay greater attention to the benefit of IT such as improved customer service, enhanced product quality, increased market responsiveness, and better co-ordination of buyer and suppliers in business perspective. Pereira (2002) points out that while IT helps organizations improve productivity, recent information security technology has created competitive advantage environments across all industries. For example, Brandyberry (2003) argues that managerial IT skills are rare and firm specific and therefore likely to serve as sources of sustained competitive advantage.

A quantitative approach has been chosen to best target the critical data and to explore an ambiguous relationship between business process and information security technology capability. Three sets of data are to be collected from stratified samples and processed to measure the complexities the IT and business objective alignment. The subsequent analysis of the findings can provide a framework in which the levels of acceptable variation may be determined and the consequences of variations defined. In this research triangulation is used to enhance the data range and to invite reflection on the complexities of a troublesome relationship. According to Henderson and Venkartraman (1991), effective management of IT requires planning processes that create a high degree of alignment between the business and IT strategies. They argue that the inability to realize value from IT investments is, in part, due to the lack of alignment between the business and IT strategies of organizations. Luftman & Sledgianowski (2005) point out that alignment seems to grow in importance as companies strive to link IT and business through dynamic business strategies and continuously evolving technologies. This research pays attention to the linkage of information security as IT and to the potential for the enterprise to significantly affect the competitiveness and efficiency of the business. The essential issue is how information security as IT can enable the achievement of competitive advantages for the enterprise. Moreover, consideration is to be made of advice that could help an organization make more effective use of the information security technology.

1.1 ACADEMIC MOTIVATION

Information technology has become the generally accepted term that encompasses the rapidly expanding range of equipment, applications, and services used by organizations to deliver data, information, and knowledge. With the expansion of information technology capabilities, users' roles in information systems have evolved from IT specialists for access information facilities, to non-IT personnel for regular operation, to unspecified individuals from outside. He et al. (2000) pointed out that with the serious threat of unauthorized users on the Internet, information security is facing unprecedented challenges, and effective information security is one of the major concerns. This study focuses on the effective and efficient utilization of information security as IT, and the business perspective on information security technology. In the literature reviewed, the evaluation of the information security role focused on security technology effectiveness measures, for example systems usage, cost/benefit analysis, user satisfaction, information economics, and system capability. However, the information security function also includes protection of information and improving data processing

(Broderick, 2001). According to Kearns & Lederer (2003), organizations continue to question the benefits of information security technology in conjunction with new corporate initiatives such as business process, e-commerce, and enterprise resource planning. Zehir & Keskin (2003) have noted that business today requires effective information security across a wider scope of variables than that of the traditional IS, and often linear, information security measurement, to achieve understanding of the factors that create the foundations of future success. It is important for this thesis to establish a comprehensive view of information security measures that indicate the overall improvement of business productivity, which can then be more fully aligned with organization goals and business competitive advantages.

A range of business improvement models have been developed which can act as catalysts for developing and aligning measures and strategy (Ackroyd, 2002; Lee & Menon, 2000; Mahmood & Mann, 2000). A model such as the balanced scorecard (BSC) is seen a tool to enable the alignment of measures and strategy in a dynamic manner (Kaplan and Norton, 1999). Grembergen (1999) applied the BSC to the IT domain and introduced the concept of the cascading balanced score card. This model can be used to monitor and control the characteristics essential to the future success of the organization and is able to look forward, rather than relying entirely on traditional measures that are historical in nature. In the IT strategic literature reviewed, the strategic use of information technology makes a powerful impact on a business as it is transformed (Luftman, Lewis, & Oldach, 1993). According to Luftman & Sledgianowski (2005), the strategic use of information technology is a fundamental issue for every business. In essence, IT can alter the basic nature of an industry. The effective and efficient utilization of information technology requires the alignment of IT strategies with business strategies (Henderson & Venkatraman, 1993). The alignment or fit of information technology with the business is fundamental to the notion of transformation. Luftman & Brier (1999) suggest that the appropriate utilization of information technology throughout the organization should be established as an explicit requirement for acceptable performance. Devaraj & Kohli (2002) argued that the objective of information technology is not merely to solve the operating problems of a particular department. Organizations should focus on IT can strengthen the competitive performance of the enterprise (Henderson & Venkatraman, 1999).

1.2 IT BUSINESS MOTIVATION

Information systems scholars have adopted diverse conceptualizations of information technology, extending beyond hardware and software to include a range of contextual factors

associated with its application within organizations (Markus & Robey, 2004). Buyukozkan (2004) points out that the diversity exposes how underlying assumptions about what constitutes IT and what assumptions shape people's accumulated knowledge in organizations, and what constitutes a successful performance. Devaraj & Kohli (2003) argue that understanding how IT has been conceptualized in prior research also provides a firm foundation from which to derive a systematic and theoretically based definition of information technology for model derivation.

There are conceptualizations of the IT artefact that have been adopted in IS research (Orlikowski & Iacono, 2001). In the first conceptualization, IT is viewed as an engineered tool that does what its designers intended, for example, productivity enhancement and reshaping social relations. Such a view is frequently used within IT business value research, i.e., IT is assumed to be a tool whose intended purpose is to generate value. Second in the proxy view, IT is conceptualized by its essential characteristics, which are defined by individual perceptions of its usefulness or value, the diffusion of a particular type of system within a specific context, and its investment or capital stock denominated in financial units. IT business value researchers often adopt this conceptualization in empirical studies using measures such as capital stock denominated in dollars. The ensemble view is the third conceptualization, focusing on the interaction of people and technology in both the development and use of IT. Case studies examining IT business value within specific organizations often adopt the ensemble view (Kraemer, Dedrick, & Yamashiro, 2000; Williams & Frolick, 2001). In addition, as quantitative IT business value research has evolved beyond examining the productivity paradox (see chapter 3) of low aggregate productivity growth during a period of high IT spending, it now explores how firms use IT to generate value. Researchers have begun to incorporate the role of organizational co-innovations such as workplace practices (Brynjolfsson, Hitt, & Yang, 2002). As the emphasis of the fourth view is on algorithms and systems development and testing as well as data modelling and simulation, it is less applicable to IT business value research. The final conceptualisation group is studies adopting the nominal view that invoke technology in name but not in fact. An example is the derivation of a two-stage game analyzing the impact of IT application on total factor productivity in the context of oligopolistic competition, which introduces IT solely via its posited impact on cost reduction and product differentiation (Belleflamme, 2001).

Examining conceptualizations of IT by IT business value researchers reveals that prevailing assumptions have delimited accumulated knowledge in three principal respects.

First, IT is frequently operationalized using aggregate variables measured in dollars or counts of systems (proxy view), limiting understanding of the differential impacts of alternative types of IT as well as the role of usage (Belleflamme, 2001). Furthermore, software is often treated implicitly via assumptive measures or sometimes omitted entirely from the analysis. Given evidence of its association with firm performance (Hitt, Wu, & Zhou, 2002), there is a need to incorporate software when conceptualizing IT. Also, IT is frequently assumed to lead to an outcome intended by managers (tool view), limiting understanding of unintended consequences (Markus & Robey, 2004). Similarly, the treatment of the role of IT employees is unsystematic and often excluded from the analysis (ensemble view), hindering understanding of the role of IT management and technical expertise in generating IT business value. When included, IS employees have been incorporated in an additive fashion with IT stock (Hitt & Brynjolfsson, 1996) as a separate construct that is complementary to IT (Black & Lynch, 2001), or conceptualized as being inextricably intertwined with IT within business processes (Kraemer et al., 2000). The problem is exacerbated by increasing adoption of networked systems spanning multiple organizations and hence multiple IS stakeholder groups.

1.3 PROBLEM AREA

According to Bharadwaj (2000), the complex problem of linking IT to business process is informed by the insights of multiple theoretical paradigms. However, Johnson (2004) argues that the absence of a unified theoretical framework has led to a fractured research stream with many simultaneous but non-overlapping conversations. Other researchers have taken an alternative approach in modelling IT business value by focusing on the attributes of IT and other organizational resources that together may confer a competitive advantage (Porter & Stern, 2001). Porter (2001) points out that IT is widely available to all enterprises and can only confer a sustainable competitive advantage if it is applied to leverage differences in strategic resources. Only IT management skills may lead to sustained competitive advantage, and they acknowledge that "there may be other attributes of IT whose competitive implications have not been fully evaluated" (Johnson, 2004, p. 251). The central problem is hence the complexity of the context and the difficulty of identifying the relevant relationships within the context. Claims for causal relations and net effects all require qualifying and reference to the relative trade-offs with attributes that have not been measured. The problem comes back to identifying the causal factors of competitive advantage.

Owen et. al. (2001) derived a resource-based conceptual framework mapping the attributes of IT to competitive advantage. According to the framework, the extent to which IT is valuable, heterogeneous, and imperfectly mobile determines the level of competitive advantage (Owen et al., 2001). This proposed study is to examine security as IT in relation to competitive advantage. The research objective is to develop a model of information security within the business value generating process. The aim is to develop a conceptual model that is not only based in theory, but also rooted in one that is inherently suitable for analyzing the complexity of IT in business processes. Ideally, it will embrace effective security while enabling consideration of the rich contextual processes associated with managing IT for business value. This identification of the problem then leads to the research question (see Chapter 4, pp. 113, 115).

1.4 THE RESEARCH QUESTIONS AND HYPOTHESIS

The central focus of this research is information security in business organisations and the most obvious (visible) way to study information security is to identify a common artefact that is embedded within the IS contexts. The area of study consequently has two distinct domains of knowledge: the computer IT knowledge, and business organisation knowledge. A review of the literature (above) revealed that studies examining the association between information security technology and business processing are divergent in how they conceptualize key constructs and their interrelationships. Previous research has shown that information security technology may indeed contribute to improving and protecting of information systems of the enterprise (Brynjolfsson & Hitt, 1998; Burnham, 1999). Moreover, the dimensions and extent of IT and business depend on a variety of factors, including the type of IT, management practices, and organizational structure, as well as the competitive and macro environment (Haughwout, 2000; Willcocks & Graeser, 2000). In the literature reviewed, chapter two defined the IT context in relation to computer network security performance and design, and the associated issues and problem areas. In chapter 2, a key linkage between business and IT professionals is found in the seamless utilization of security technologies. For example, security capablities of IT were greatly enhanced between IPv4 and IPv6. In particular the protocols for Virtual Private Networks (VPNs) were enhance for greater business confidence (the perception of secure environments). In IPv6 the ease of use was improved, security (IPsec protocol) refined and routing options increased. As pointed out by Younglove (2001) VPN functionality is a key software for securely connecting enterprise networks over a public network infrastructure, and VPN is a generally accepted business technology. A VPN is an

especially effective means of exchanging critical information for employees working remotely in branch offices, at home, or on the road. It can securely deliver information between vendors, suppliers, and business partners, who may have a huge physical distance between them. Zhang et.al. (2003) states that such networks are deployed within a public network and aim at providing a private working environment to its users. The VPN is a key technology linkage between the worlds of IT and business and a focused context for research
.

In chapter 3 the literature relating to the business perspective of IT and the business value extraction from the business perspective was reviewed. A key problem area identified from the literature was the alignment of IT and Business objectives, and the subsequent organisational consequences for systems security. The review focused on the linkage of information security within the enterprise and the competitiveness of the business. The debatable issue was the extent to which IT contributed to the organisational performance and the established research supported claims either for or against IT playing a significant role in organisational performance. Sledgianowski & Luftman (1996) pointed out that alignment seems to grow in importance as companies strive to link IT and business in light of dynamic business strategies and continuously evolving technologies. According to Venkatraman & Henderson (1993), effective management of IT requires planning processes that create a high degree of alignment between the business and IT strategies. They argue that the inability to realize value from IT investments is, in part, due to the lack of alignment between the business and IT strategies of organizations. The literature reviews positioned IS protection (security) as a concern that was discussed at both the IT and business management levels. Security was a common factor that ranked highly in research reports (as above) and in all of the literature a critical success factor for enterprise success.

The nexus of competing interests formed one axis in the reviewed literature to evaluate organisational performance. This was commonly termed the alignment issue. However, all the reports reviewed consideration was made of the wider IS context. IS were seen (the more recent literature) as parts of a bigger whole, usually termed the enterprise system. As a consequence the technical and interest contexts were important but not the only factors influencing enterprise effects. For example, consideration of human (or soft) issues also provided grounds to establish contributing factors. Thus a research question requires positioning within the enterprise system context, and a set of sub-questions developed so that the contextual issues are suitably investigated before hypothesis testing may occur. The key

learning from the literature is that interaction occurs at many levels in an enterprise research field.

A simple starting position for an investigation into IS protection is to start with the desired organisational effect and then backward map into the factors and their variables. Such an approach reverses standard quantitative methodology but the reviewed IS literature suggests that a variety of approaches are allowable providing they are justified and comply with ways of establishing reliability and validity (as above). Hence a desired enterprise effect would be a secure (protected) IS. However, such simplicity overlooks that a secure (protected) IS may be inappropriate (unusable) by people within the organisation. The qualification comes from the literature (reviewed above) that determines seamless security to be the desired organisational effect. Hence a stronger starting position would be the identification and selection of an IS cultural artefact, and then the measurement of properties of the artefact in relation to the desired effect. The proposal of this study is to investigate the application of VPN (the cultural artefact) technology in the business context (both practical and theoretical), and from this research provide informed advice for effective information systems security (protection).

The research question that brings together the matters discussed above is:

What are the competitive advantages for business enterprise of Virtual Private Network Security?

This question provides a bridge between the worlds of IT and Business interests, and targets the possibility of identifying factors in a seamless secure systems design. Critically the human and the interest factors are linked to the technical factors (discussed above). However, to drill further into the context and to identify possible relationships and interaction factors a set of sub-questions are required. The key relationships between the VPN artifact and the systems environment can be grouped into (a) work systems links, (b) IT systems security expectations, and (c) business systems competitive advantage expectations (as discussed in Chapters 2 & 3). The set of sub-questions for each of the groups that can identify specific classes within the systems are as follows:

(a) What measures are critical for MIS security?

Studies responding to this question focus on identifying, measuring on information security, or estimating perspective of using Virtual Private Network (VPN) between business and IT in organization.

(a) In what ways can a more efficient computer security system benefit the overall organisation competitive advantage?

This is to examine if efficiency information security can be associated with the competitive advantage as perceived by the organization's business processing. In other words, efficiency information security can protect and secure data which allow organization to have secure environment and improve business processing.

(a) What elements are required in the MIS to assure protection?

This question is focus elements of MIS protection. Information security is becoming the most critical information technology-related challenge they face. Information security has many different facets, but the main goal is protecting the confidentiality, integrity, and availability of an organization's information assets.

(b) What is the relationship between IT and Business objectives for optimal security assurance?

This question is find out the big picture of information security as objective of business and IT in their current organization, to make linkages between different organizational units, and ensures focus on a larger perspective needed to extract benefits from the potential fit between the business and IT within the organizational context. It represents a holistic view of the organization and its current activities.

(b) In what ways can the VPN improve the performance of the employees and managers in an organisation?

This question is seeking evidence in support of the existence and performance effects of using VPN by employee and managers as information security technology. While it may be appropriate to impose consistent IT strategies and consistent information security technology solutions onto business units operating in different industries, it is better to use common information security technology and to coordinate the strategic IT decisions of the business units by using common IT strategy making, IT human resource management, and IT vendor management processes.

(b) What intangible MIS elements contribute to business value delivery?

This question is to investigate the contribution of MIS as business value. Management Information Systems are distinct from regular information systems in that they are used to analyze other information systems applied in operational activities in the organization.

(c) What is the relationship between MIS security and competitive advantage?

This question is to exam the relationship between MIS security and competitive advantage. In literature, researcher interests in protecting MIS system and competitive advantage. The focus of this question is the relationship between MIS security and competitive advantage.

(c) In what ways can VPN provide cost advantage?

This question is to exam cost advantage of VPN. If VPN enables enterprises to contain costs, enhance security, and expand access and availability, while enhancing their business processes and improving customer service and best practices.

(c) What organisational capabilities are enhanced by effective MIS security?

A set of asserted hypothesis can be similarly developed from the reviewed literature. An assumption that underlies the literature is that business objectives and IT objectives are different, and in some way are causal with regard to conflict and the smooth running of enterprise systems. Hence a working hypothesis is framed as:

H1: There is no significant difference between business and IT objectives.

Studies examining the objectives between business and IT who use VPN for their business process, profitability improvement, cost reduction, competitive advantage, inventory reduction, and other measures of performance his may be at the functional level but the asserted consequences are strategic. This is to test if there is significant difference between business and IT objective.

H2: VPN usage has a significant effect on business competitive advantage.

This Study is examining the deployment of VPN within organizations to protecting MIS system and gain business competitive advantage.

H3: VPN usage has a significant effect on MIS protection.

The literature on IT and organisational performance left no doubt and little evidence that alignment is a key issue. The relationship is generally asserted and requires testing.

H4: IT objective alignment can significantly improve business performance.

This is to test if IT objective alignment can significantly improve business performance in organization. If this study provides a detailed account of the role that IT professionals play in the creation and sharing of organizational knowledge within the context of information security technology.

H5: Business objective bias can significantly predict systems capability.

This is to examine business objective bias can significantly predict systems capability. This is to predict VPN as information security technology which has used by business people.

H6: The variation between IT/Business objectives can significantly predict systems capability.

Finally, this is a hunch but a plausible conjecture from the literature review, that good security is a predictor of systems capability in the business context:

H7: MIS security can significantly predict organisational competitive advantage.

Figure 4.3 provides a data map of these inter-relationships defined above. The selection of data types and the actual survey questions (defined in the following sections) are also included to provide a complete overview of the potential data collection field and the subsequent data analysis framework. The sequential Phase analysis is also defined in the concluding sections below.

1.5 STRUCTURE OF THE THESIS

The remainder of this thesis is organized as follows. In chapter 2 the IT context is specified to define the important business information system (BIS) elements that impinge on information protection. Networks are defined in terms of the fundamental communication models and the ways of communicating business information across networks (routing). These BIS elements are then carefully evaluated to identify the risks associated with each and to identify the inherent weaknesses in any BIS. Table 2.1 provides a summary of the analysis. Virtual Private Networks (VPN) are then selected as a generic and core BIS protection technology. The VPN IT context is specified in detail and analysed for the information protection capabilities.

In chapter 3, the central problem area and relationship of security as IT to business is addressed. Key literature is reviewed to locate the views others have regarding the relationship of business and IT, and competitive advantages. The issues of extracting business value from IT, business performance, the linkage relationship, the strategic relationship, IT Governance, and ISO / IEC security standards are documented. The role of IT has changed in business and how organizations have reacted to this change is noted. The major transition point in organizations' usage of IT is identified on a time base in order to provide a chronicle of events, placing current opportunities in a developmental context. Overall Chapter 3 is a comprehensive review of the IS literature in relation to the proposed research problem area.

In Chapter 4 a methodology is specified to best answer the research question (see p. 113). Sub-questions and hypotheses are also specified (see p. 115). The concern for a research approach that can address the complexity of the context of the problem is addressed by adopting and developing a triangulated hybrid approach that requires different data type to be collected. Previous related studies are reviewed and used to instruct the design. The proposed field study is in three large and geographically disperse international enterprises with a stratified (role based stratification) sample of 40 participants from each location. The

selected power function was 80% and the triangulation of different data type allows audit of different perspectives in the enterprise systems.

Chapter 5 reports the findings. The problems in the field and the response rates are addressed. Variations to the research plan in Chapter 4 are acknowledged and explained in Chapter 6. The chapter is divided into the three independent phases of analysis. These phases corresponded to the different data type that were collected and the unique three sub-questions that related to each data type. Each subsection is structured to first report the overall findings, the business – IT strata analysis, and in conclusion a summary of evidence (a table) that links the findings to the sub questions. The triangulation is then completed and the evidence for and against the hypotheses compiled.

In chapter 6 the findings reported in Chapter 5 are discussed and explained in terms of the theoretical framework developed and the pervasive problem area. Each phase is revisited and the links between the business and IT professional debated. Finally, the results and the implications of the study are presented and some limitations and concluding comments offered.

Chapter 7 gives an integrated discussion about the research findings and the links to possible further research. The case for more hybrid studies and studies that use a range of data type is made.

Chapter 2
THE IT CONTEXT

2.0 INTRODUCTION

Business Information Systems (BIS) are deployed within and between organisations to manage the information requirements of customers both internally and externally (Alter, 2002, p.17). The notion that a BIS is integral to strategic activities is advanced by a number of writers (for example, Gates, 1999; Luftman, et al. 2004; Oz, 2006). The argument is that IT and business processes are inextricably related to the point where "the immediate availability of accurate information changes strategic thinking from a separate, stand-alone activity to an ongoing process integrated with regular business activities" (Gates, 1999, p. 15). In Chapter 2, the BIS is reduced to its IT components in order to identify the IT contribution and to contrast this with the reduction of the BIS to its strategic business components in Chapter 3. A system is more than the sum of its parts (Severance & Passino, 2002) and composed of many subsystems that inter-relate for the overall business effect. The Management Information System (MIS), for example, is a sub-system within the BIS that is critical in the strategic business context and has the effect of supporting and controlling management decision-making (Mahmood & Mann, 2000). The purpose of this chapter is to define the IT components of the BIS in relation to a generalised BIS IT capacity and to locate the critical IT elements in relation to securing information within a BIS. Chapter 3 that follows is to resolve the business components and in particular the contribution the MIS makes to business effects.

The fundamental IT structure for the BIS is the network (Cohen & Kaempfer, 2000). Networks provide the capacity for the exchange of information and are composed of sub-systems, elements and components (Burnham, 1999). The Virtual Private Network (VPN), for example, is a network within a network that achieves the business effect of secure information transfer (the complexities and importance of this network will be defined and discussed later in this chapter (Yuan & Strayer, 2001). The definition of network within BIS however is undergoing constant change. The definition is both theoretical and pragmatic, and both definitions of the word have changed as new capacities, architectures and applications have evolved over time. This is more than simple sematic differences. A network today is a very different construct than one at another point in history. Different perspectives have also influenced how a network is to be defined. In the last decade the availability of IPv6 standards (Kindred & Sterne, 2001; H. Lee & Eom, 2001) and the preoccupation of

businesses with protecting information assets (Gelinas et al., 2004; Shin, 2003; Willcocks & Graeser, 2000) have altered not only the definition of BIS but the relationship of the IT and business interests in an organisation. This is the issue raised by Gates (1999) and others above that locates an uncertainty as to where and to what a BIS relates in an organisation. Clearly the BIS is critical to business effects but the ownership and the creation of the effect is less certain. The matters of competitive advantage or business performance are ambiguously related to different bases in literature, and different studies isolate different critical success factors, correlates, determinants, and relationships for key performance indicators.

Key questions arise as to the relationship between business and IT interests in a BIS that have consequences for systems coherence. In this chapter the BIS is to be defined in terms of its central IT components and the relationship of IT to a key BIS outcome, that of information security. The chapter is structured to briefly overview the scope of a BIS and its sub-systems, and then to look directly at the critical IT components that make a BIS. The first section reviews network. The fundamental building blocks of IT network are defined and then discussed in the context of more recent changes to protocols and the subsequent implications for BIS capacities. The issue of architecture and its bearing on the definition of network is elaborated in section 3 by identifying the VPN sub-network. The relationship between VPN and the protection of BIS is also a key element in the architecture of BIS and the forecasted future development of BIS designs. The relationship between IT design and business requirements, and IT capacities and business value are addressed in Chapter 3. The relationship between IT and information asset protection is taken up in the last section of this chapter in a review of BIS concerns, a review of various IS security models and a definition of information protection. The section also explains in more detail how security concerns in organizations regarding the internet and different types of information asset attack can be mitigated.

2.1 BUSINESS INFORMATION SYSTEMS

A business information system (BIS) is an information system (IS) that specifically provides the information resource for business activities. It is different from for example a manufacturing information system, because a BIS is specifically concerned with the business model. The BIS inter-relates with many other IS from the specific business perspective. The BIS is composed of many different subsystems, such as the management information system (MIS), the expert information system (EIS), and so on (Casper, 2000). These sub-systems

may be strategic, tactical, or operational and interact internally or externally to deliver an information resource, for example, to the executive information system. BIS are composite work systems (Alter, 2002) that function within the business context and are designed to meet the business objectives. These systems are mission critical and influence the competitive capacity of a business (Severance & Passino, 2002). The interest of this research is to identify the systems components that most influence the business effect and to understand the diversity of interaction within a BIS that leads to secure information systems.

The BIS is composed of different layers of elements that inter-relate for the overall business effect. For example, data is a critical element of the BIS but data requires capturing, storage, transmission, processing, and protecting. These actions occur at different layers in a system so that the capturing comes at a point of sale (POS) where there is an interface of customer and business, and customer and IT. The data is processed and transmitted in an IT layer that includes hardware, software and network. Data is stored in a database that is in part software and in part hardware. The data is extracted from a database for business purposes by different business IS (for example, MIS, EIS, and so on) and used for different business purposes. In another layer a business model has determined the business objectives and design of the business architecture and this layer interfaces and inter-relates with the IT layer. The BIS structure is rationalised into a three-layer model for effective business architecture (Kalatoa & Robinson, 2001, p.106). The top layer above the layers of infrastructure and info-structure is the business design. The lower two layers represent increasing complexity from fundamental IT requirements, such as reliability, security, and data bases, to the middle layer that houses a variety of applications for the co-ordination of customer relationship management, supply chain management, financial control, and so on (Sirisuka & Cusack, 2003, p.2). The layers are separated into hardware, software, and business objectives.

The relationship of business and IT is a critical issue in the definition of the BIS. The three layer business model controls the relationship by giving the business leadership at the upper layer in the definition of the business design and the IT people leadership at the lower layer in the definition of the IT support. However, the issue surfaces for debate in the middle layer where the business objectives interface with the IT objectives and common ground has to be negotiated for business effectiveness. It is in this layer that business and IT models are brokered and that abstractions for the IT and business relationship implemented. This chapter is concerned with defining the IT context of BIS and hence the key elements relating to the IT protection of information assets are reviewed in this section. The elements of network, routing and architecture are defined within the BIS context.

2.1.1 Networks

Formalized study has produced volumes of works on the topic of network design. The general concepts of relatedness and connection are used to define a network, and then terms such as layers, protocols and architecture are used to define the specifics of a network. A set of layers and protocols, such as in the TCP/IP model, is called network architecture (Ross & Tittel, 2001). Heuring et.al., (2003) point out that the specification of architecture contains enough information to allow implementers to write programs to drive the hardware for each layer. Forouzan & Fegan (2003) argue that to reduce the design complexity, most networks are organized as a series of layers, each one built upon the one below it. The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network (Ross, 2001). However, in all networks, the purpose of each layer is to offer certain services to the higher layers, shielding those layers from the details of how the offered services are actually implemented.

The two most widely accepted network reference models are the OSI (Open System Interconnection) seven-layer model, and also the TCP/IP (Transmission Control Protocol/Internet Protocol) four-layer model (Stallings, (2000b). The problem solved by these conceptual models is that of connecting different layers to create the overall effect of network communication (FitzGerald, 2002). The solution is that every layer needs a mechanism for identifying senders and receivers (Davies & Lee, 1999). Stallings (2000a) further argues that since a network normally has many computers, some of which have multiple processes, the central problem is to secure object-to-object identification and secure packet exchange. The design and development of a network system has embedded structure that provides minimum technical requirements (Main, 2004) leading to business attributes such as security, being under developed in most models. The objective in the following sections and subsections is to review the structural contribution to network of the OSI and TCP/IP models, and then to identify the problem areas that are left open and have implication for BIS network security.

2.1.1.1 The OSI Model

In the late 1970s, Tudor (2000) claims that there were two projects for the architecture of networking systems. According to Stallings (2003), the International Standards Organization (ISO) had administered one for standardization, while another one was undertaken by the International Telegraph and Telephone Consultative Committee, or CCITT (the abbreviation is from the French version of the name). These two international standards bodies each

developed a document that defined similar networking models. By 1983, the two documents were merged together to form a standard called the Basic Reference Model for Open Systems Interconnection (Forouzan et.al., 2001; Panko, 2000). Ross et.al. (2003) state that the standard is usually referred to as the Open Systems Interconnection Reference Model, the OSI Reference Model, or even just the OSI Model. It was published in 1984 by both the ISO, as standard ISO 7498 and CCITT.

The original objective of the OSI was not to create a model primarily for security purposes. The OSI Reference Model was intended to serve as the foundation for the establishment of a widely adopted suite of protocols that would be used by international internetworks. Tanenbaum (2002) states that the idea behind the OSI Reference Model was to provide a framework for both designing networking systems and for explaining how they work - including setting up networks and connecting them together. He emphasized that the OSI Reference Model represented an early attempt to get all of the various hardware and software manufacturers to agree on a framework for developing the multiplicity of networking technologies. According to Wetteroth (2001), the OSI model is primarily theoretical, and that networking protocols are not always designed to fit strictly within the confines of layers. The usual stated reason for this is that "the OSI model is too theoretical and does not apply to modern networking protocols like TCP/IP" (Wetteroth, 2001, p. 139). The fundamental assumptions of the OSI model were that communications could be standardized in to vertical connectivity for control and stratified into layers for functionality (Gann, 2000). Forouzan & Fegan (2003) argue that the strength of the OSI model is its hierarchical organization of complexity, the adoption of independence functionality layers, and the consequential direct control of the lowest level of computer functionality by Application objects. A summary of the OSI layers below defines the fundamental IT building blocks for a BIS network, and the security implications of each layer are discussed in Sub-Section 2.1.3 (see figure 2.1).

Layer 7	**Application**
Layer 6	**Presentation**
Layer 5	**Session**
Layer 4	**Transport**
Layer 3	**Network**
Layer 2	**Data Link**
Layer 1	**Physical**

Figure 2.1 OSI Model (Tanenbaum, 1996, p. 36)

The Physical Layer (1) is concerned primarily with transmitting data bits (0 or 1) over a communication circuit (FitzGerald, 2002). Typical questions here are how many volts should be used to represent a 1 and how many for a 0, and how many microseconds a bit lasts. Also whether transmission may proceed simultaneously in directions, how the initial connection is established, how it is terminated, and how many pins the network connector has and what each pin is used for. The layer has to deal with mechanical, electrical, functional, and procedural interfaces, and the physical transmission medium, which lies below the physical layer.

The Data Link Layer (2) is concerned with the logical elements of transmissions between two directly connected stations (Panko, 2000). The main task of the data link layer is to take a raw transmission facility of the layer below and transform it into a line that appears free of transmission errors in the network layer above (Davies & Lee, 1999). It accomplishes this task by having the sender break the input data up into data frames (typically a few hundred bytes), transmit the frames sequentially, and process the acknowledgment frames sent back by the receiver. Since the physical layer merely accepts and transmits a stream of bits without any regard to meaning of structure, it is up to the data link layer to create and recognize frame boundaries. This can be accomplished by attaching special bit patterns to the beginning and end of the frame. If there is a chance that these bit patterns might occur in the data, special care is taken to avoid confusion.

The Network Layer (3) performs addressing and routing. Its key function is to provide information for routers to make decisions (FitzGerald et.al., 2000). Forouzan & Fegan (2001) have noted that this layer typically uses constructs such as IP addresses to identify nodes, and routing tables to identify overall paths through the network and the more immediate next-hop that a packet may be forwarded. Protocols such as ARP (Address Resolution Protocol) facilitate that process, giving layer two mapping to layer three addresses, and telling layer three what link-layer path should be taken to follow its routing table indication of the appropriate path. In the opposite direction, protocols such as IP will identify their higher-level layer four transmission protocol such as TCP (Transport Control Protocol) or UDP (User Datagram Protocol) in order to direct layer four as to how the incoming data should be handled (Tanenbaum, 2002). Routers control the operation of the combined layers, 1, 2, and 3 by coordinating the vertical processes.

The network layer (3) is the last layer that has a rough physical correspondence to the real world. Landwehr (2001) states that a given host will typically have a single layer three

address or single layer three address per interface. “This tends to make layer three addressing critical not only to network topology but also to node identity” (Landwehr, 2001, p. 3). According to Lee & Jones (2001), the layer three address is the primary qualifying value in a filtering rule, with some rules using them as a sole identifier. Layer three addressing is also used by applications to identify resources, using DNS (Domain Name System) resolution to map a hostname to an address or group of addresses. Layer three protocols often have mechanisms for broadcast or multicast of data to multiple machines in finite or arbitrary scopes (Lee & Jones, 2001).

The Transport Layer (4) provides host-to-host or end-to-end connectivity by establishing, maintaining, and terminating logical connections for the transfer of data between end users (Held et.al., 2002). Choi et. al. (2003) assert that transport protocols may be designed for high reliability and use mechanisms to ensure data arrives complete at its destination, using for example, the TCP protocol. Protocols may choose to reduce overhead and simply depend upon the best efforts of the lower layers to deliver the data, and the protocols of the upper layers to ensure success to the levels they require, with for example, the UDP (User Datagram Protocol) protocol. Transport protocols may implement flow control, quality of service, and other data stream controls to meet their transmission needs.

The Transport Layer (4) is the first purely logical layer in the OSI model. Caloyannides (2003) states that it is the primary point where multiple data conversations from or to a single host are multiplexed. Some transport protocols such as TCP (Transport Control Protocol) and UDP (User Datagram Protocol) use the concept of port numbers to allow multiple simultaneous conversations between numerous destinations to individual local protocols or applications. Other protocols such as ICMP (internet control message protocol) rely on higher-layer data to sort out multiplexing (Caloyannides, 2003). Because the transport layer is where data conversations to a given host are multiplexed and sorted, it is often used as the primary means of service identification within a given host, much as how layer three addresses are used to identify service locations within the context of the entire network (Ross et.al., 2003).

The Session Layer (5) allows users on different machines to establish connection for communication (FitzGerald et. al., 2000). A session allows ordinary data transport, as does the transport layer, but it also provides applications execution. A session might be used to allow a user to log into a remote time-sharing system or to transfer a file between two machines. One of the services of the session layer is to manage dialogue control. Sessions can

allow traffic to go in both directions at the same time, or in only one direction at a time. If traffic can only go one way at a time, the session layer can help keep track of whose turn it is.

The Presentation Layer (6) deals with the organization of data passed from the application layer into the network. This layer allows for the standardization of data and the communication of data between dissimilar hosts, such as platforms with different binary number representation schemes or character sets (ASCII verses UNICODE for example) presentation layer protocols typically rely upon a standardized data format for use on the network, and various conversion schemes to convert from the standardized format into and out of specific local formats (Forouzan & Fegan, 2001). The Presentation Layer can also control network-layer enhancements such as compression or encryption.

The Application Layer (7) is the end user's access to the network. The primary purpose is to provide a set of utilities for application programs (Stallings, 2004). The application layer contains a variety of protocols that are commonly used for linking many different and often incompatible terminal types. The solution provided by application is to define an abstract network virtual terminal for which editors and other programs can be utilized. To handle each terminal type, a piece of software must be written to map the functions of the network virtual terminal onto the real terminal. For example, Stallings (2004) points that when the editor moves the virtual terminal's cursor to the upper left-hand corner of the screen; this software must issue the proper command sequence to the real terminal to get its cursor there too. All the virtual terminal software is in the application layer.

2.1.1.2 The TCP/IP Model

TCP/IP was initially developed in the 1970s as part of an effort to define a set of technologies for operating the fledgling Internet (Jones, 2002; Ritchey et.al., 2002). The Transmission Control Protocol/Internet Protocol (TCP/IP) was developed for the U.S. Department of Defense's Advanced Research Project Agency Network (ARPANET) by Vinton Cerf and Bob Khan in 1974 (Dennis, 2002). Black (2000) points out that the name TCP/IP came about when the original Transmission Control Program (TCP) was split into the Transmission Control Protocol (TCP) and Internet Protocol (IP). The first modern versions of these two key protocols were documented in 1980 as TCP version 4 and IP version 4 (Yoke, 2002). It provided the basic datagram delivery capabilities for TCP/IP functions, and it has proven its quality in use over a more than two decades. In the last decade, development of a new version of IP has been underway, officially called Internet Protocol version 6 (IPv6) and also sometimes referred to as IP Next Generation or IPng. IPv6 is available to take over from

IPv4, and will be the basis for the Internet of the future (Nicolle, 2001) (See section 5.1 and 5.2 for a detailed definition of IP version 4 and 6).

The OSI reference model was the forerunner of later developments included in the TCP/IP model. The TCP/IP model was a practical solution for worldwide internetwork growth and development. The four TCP/IP layers, built on top of a hardware layer, have to date proven sufficient for practical purposes (Mansfield, 2003). The session and presentation layer functions defined in the OSI model are "omitted from the TCP/IP model, and the functions are fulfilled as needed by different TCP/IP protocol" (Tanenbaum, 1996, p. 36) (See Figure 2.2).

Layer 4	**Application**
Layer 3	**Transport**
Layer 2	**Internet**
Layer 1	**Host to Network**

Figure 2.2 The TCP/IP Model (Tanenbaum, 1996, p. 36)

IP provides functionality to allow different types of networks on an Internet, and the TCP provides reliable data transfer. The two lowest TCP/IP layers deal with the world of device drivers, media access controls, physical attachments, and physical signals (Jones, 2002). The two lowest layers package data into units, frames or packets, and send the data from an interface on the local system to a destination interface attached to the same physical network (Mansfield 2003). Local area networks (LANs) and wide area network (WANs) provide these lower layer functions. The boundary between IP and the lower layers is an important one. When a vendor implements this boundary a new type of network interface and medium for IP can be added to computer without undue effort (Mansfield, 2003). IP can share a network interface and medium with other protocols.

The Host-to-Network layer (1) interfaces the TCP/IP protocol stack to the physical network. The TCP/IP reference model does not specify in any great detail the operation of this layer, except that the host has to connect to the network using some protocol so it can send IP packets over it (Davies & Lee, 1999). TCP/IP does not specify a particular protocol here and can therefore use almost any available network interface, including a device driver for maximum flexibility. The Host to Network layer (1) of TCP/IP provides global addressing and routing of packets between network segments. Caloyannides (2003) notes the source and destination IP addresses of the packet are specified at this layer. The Transport

layer controls the flow of data between different host services, which are addressed by a local port number (Caloyannides, 2003). TCP/IP offers two transport protocols. The Transmission Control Protocol (TCP) is stream oriented and provides a reliable, byte oriented data flow through control functions that are largely transparent at the Application layer. The User Datagram Protocol (UDP) is record oriented and simply offers the ability to send packets between hosts, so the application must provide control functions if reliable delivery is required (Ritchey et al., 2002).

The Internet layer (2) delivers data across the various physical networks that interconnect a source and destination machine. Routing protocols are closely associated with this layer. The message unit in the Internet layer is called an IP datagram (Forouzan & Fegan, 2001). The datagram is the packet format defined by Internet Protocol. The first five or six 32-bit words of the datagram are control information called the header. The header contains all the information necessary to deliver the packet.

A transport layer (3) is the interface between the application layer and the complex hardware of the network (Ross, 2001). It is designed to allow peer entities on the source and destination hosts to carry on conversations. Transport layer manages the flow of data between two internetwork hosts. TCP/IP relies on two transport protocols, TCP (Transmission Control Protocol) for reliable data flow, and UDP (User Datagram Protocol). Transmission Control Protocol (TCP) is a reliable connection-oriented protocol that allows a byte stream, originating on one machine, to be delivered without error on any other machine (Ritchey et. al., 2002). It fragments the message into discrete packets and passes them onto the Internet layer. When packets are being sent out, not all of them will take the same route. This may result in packets being delivered out of sequence. TCP has a way of reordering the segments to avoid the need of the sender resending all the segments again. TCP can be compared to the telephone system. When a call is made, a direct connection is made between the two people involved in the conversation. There is a definite path for the voice data to travel along, and it is not possible for the information to be waylaid on the way.

User Datagram Protocol (UDP) is an unreliable connectionless protocol. It is useful for applications that do not require or want TCP's sequencing or flow control. It is used for one-shot, request-reply applications where prompt delivery is important. Examples of these types of applications would be DNS (Domain Name System) and transmission of speech or video (Ranky, 2000). UDP minimises the overhead associated with message transfers because no network connection is established before transmission. UDP can be likened to the postal service. A message is sent to someone else by putting the address on the envelope and

dropping it into the letterbox. UDP is similar in that it drops the datagram onto the underlying architecture, the Internet Protocol, and hopes that the message is delivered. It has no way of verifying that the datagram was delivered. It does not do any error checking and it has no way of recovering data that was incorrectly delivered.

The Application layer (4) contains protocol that implement user-level functions, such as mail delivery, file transfer and remote login (FitzGerald et. al., 2000). The original TCP/IP specification prescribed a number of different applications that fit into the top layer of the protocol stack. These applications include Telnet, FTP, SMTP and DNS (Clip, 1998). Telnet is a program that supports the TELNET protocol over TCP. TELNET is a general two-way communication protocol that can be used to connect to another host and run applications on that host remotely. FTP (File Transfer Protocol) is a protocol that was originally designed to promote the sharing of files among computer users. It shields the user from the variations of file storage on different architectures and allows for a reliable and efficient transfer of data. SMTP (Simple Mail Transport Protocol) is the protocol used to transport electronic mail from one computer to another through a series of other computers along the route. DNS (Domain Name System) resolves the numerical address of a network node into its textual name or vice-versa.

2.1.1.3 Security Concerns

The OSI (ISO 7498-1) and TCP/IP Models reviewed above were initially developed for the purpose of communication. Security was a secondary matter (eg. ISO 7498-2 development) and hence there are many areas for concern when these fundamental building blocks are used for BIS network. In this section the problem of protecting the BIS information assets is reviewed from the position of the fundamental IT elements on which all information must pass, on a layer-by-layer basis. For example, Whitmore (2001) has noted that starting from a high-level application perspective, data is sent down the stack layer by layer, each layer adding information around the originally presented data until that original data plus its layers of added content are represented at the bottommost layer as a physical medium as bursts of colored light or voltage across a wire. This permits that data to physically travel from one point to the other in the real world. Gann (2000) states that in the flow of information through the models, all layers above depend upon the physical layer to deliver the data and this is the starting point for protection. The overarching understanding is the concept of defense-in-depth (Baskerville & Portougal, 2003) that deconstructs each of the layers, examines how they interact, and constructs a protective web to secure networks, systems, applications, and

data. The following analysis looks critically at each layer of the OSI Model to identify security threats, possible controls and the level of risks at each layer.

The OSI physical layer (1) is critical to data communications. It is also the most vulnerable and changeable layer that depends on the vagaries of physics rather than the logic and organization of the electronic world. A denial of service is a circuit breaker and is "Something as simple as unplugging the power or removing a network cable that can cause untraceable havoc on a network" (Scambray et.al., 2001, p. 351). The physical realm is also the hardest to maintain an audit log or monitor (Tudor, 2000). According to Long & Long (2004), no level of logical or programmatic controls can easily detect that a host has been detached from its normal network connection and is now connecting through an Ethernet tap, which may be silently duplicating any inbound or outbound communications for eavesdropping purposes. As far as eavesdropping is concerned, physical contact may not even be necessary (Wetteroth, 2001).

Fortunately, physical security for information technology can benefit from the more general discipline of physical security in the business enterprise. Palmer (2001) claims that as the somatic components of information technology are subject to the same threats as other real assets, they are also able to benefit from the same protections that the more mundane security disciplines have implemented from the beginning of modern civilization. This means that "critical assets must be behind strong locks, with strict controls on that may pass those locks and constant monitoring, logging, and review of that access" (Sarathy & Muralidhar, 2002, p. 389). Benantar (2001b) points out that such monitoring may include video surveillance, card-lock logging of entry and exit with PIN based passwords, and even biometric validation to augment password and hardware based credentials to validate actual physical identity.

The Data Link Layer (2) has been a long-neglected area of study for information security, "lost between the physical issues of layer one and the dominating realm of the firewall in layers three and four" (Gallegos, 2004, p. 198). Black (2000) argues that this lack of attention made it an area ripe for exploitation, and some of the hottest new issues in information security have heavy involvement in layer two. Due to its interaction with a variety of media and types of hardware, this layer is critical to network compatibility and as such is heavily dependant on rigid protocol standards for interoperability (Held et al., 2002). Ross (2001) notes that this dependency can allow poorly designed standards to impede security, and make the correction of issues a ponderous and drawn-out process. For example, weaknesses were found in the encryption schema that have to date only been partially

addressed (Held et al., 2002). Held et. al. points out those weaknesses have also been found in the much-touted Ethernet switch, originally thought to be the answer to the problem of promiscuous node sniffing of network traffic because of "their learning and selective forwarding. Such switches have fallen victim to the efforts of creative hackers, who have been hard at work finding the means to circumvent this protection" (Anderson & Schwager, 2002, p. 16).

The ubiquitous control for layer (3) is the firewall and when correctly configured it will let only the necessary traffic pass through its boundaries (Evans et. al., 2004). However, Kolokotronis et. al. (2002) argues that well-thought out policies that take into consideration the problems of identity must be part of the firewall deployment. "Encryption and authentication technologies such as IPSEC can be used to more reliably identify the source of IP communications" (Kolokotronis et al., 2002, p. 166). McDermott (2000) notes that routers must have strict policies regarding their exchange of routes, and use reliable means of authentication and communication with their peers. Route filters should be applied to prevent the accidental or intentional introduction of spurious network routes (McDermott, 2000). On the Internet, Route Registries and the Routing Arbiter Database (RADB) offer the means to register route announcements (Baltatu et.al., 2000). The RADB also provides filter information that allows building of local policies to validate foreign route announcements.

Some of the key vulnerabilities found at the transport layer (4) come from poor handling of undefined conditions (Chuvakin, 2004). Patton et. al. (2000a) emphasize that many transport protocols seem to have been implemented under the belief that they would be dealing with well-behaved communication from both the upper and lower levels – which is not the case in the hostile world of the global public Internet. This means that protocols are "subjected to unexpected or deliberately perverse input or handling exploiting the more obscure protocol details and so-called impossible conditions, and as a result often have unexpected behaviour" (Patton et al., 2000a, p. 199). Camp (2004) claims that attacks such as Winnuke (Winnuke is a term for a simple procedure that malicious computer users use on other computer users on the Internet.) used an obscure and out-of specification TCP (Transport Control Protocol) flag when connecting to an open TCP (Transport Control Protocol) port on a Windows machine, and the result was an operating system crash. The behaviour of a given host when presented with TCP (Transport Control Protocol) and UDP (User Datagram Protocol) packets with varying arbitrary contents can be used to fingerprint an OS (operation system) and select more focused attacks due to differences in response between different operating systems and network stacks (McDermott, 2000).

Conventional firewalls are the most common control at layer four as well as layer three. “Firewall rules should be written to be as strict as possible regarding transport layer identity” (Cortese et al., 2003, p. 55). This means that transport layer protocols should be specified individually in rules where possible rather than permitting any communication between two layer three nodes. In terms of TCP/IP communication, this means that rules should be written applying matches for layer four protocols (Hicks, et al., 2003). Gyires (2003) suggests that stronger mechanisms are possible in layer four implementations to make session hijacking more difficult. Recent improvements in TCP sequence number assignment based on random number generation rather than arbitrary and predictable sequences have made the blind takeover of TCP sessions much more difficult (Gyires, 2003). A user’s credentials in transit over the network can often be protected but the passwords themselves are weak and subject to attack. Ye et.al. (2001) state that the session layer can exacerbate this problem by poor or non-existent logging of failed access attempts, allowing an attacker unlimited and undetected attempts to guess likely passwords, or use an even cruder technique of brute-force exhaustion of all possible or probable password strings. Mechanisms within the session layer can also be used to enumerate possible usernames to pair with such guessing and brute-force attacks (Benantar, 2001).

Identity is an issue within all layers of the OSI model and between the layers the attributes of each layer are applied as a standard for identification and authorization. In the Session Layer (5), identity is the key factor, and the main controls at this layer focus on the establishment of identity. Secure channels of user and session authentication are essential to private communications (King & Hunt, 2000). Cryptography technology allows for both the reliable identification of remote parties and the means for protecting the exchange of data from prying eyes (Younglove, 2001). Geiselmann et. al. (2003) state that passwords and other user credentials should be passed and stored in encrypted form to prevent interception or theft. User accounts should have expiration dates based on both usage and fixed time, requiring the update of credentials and reauthorization of access. Session identification may need to be based on a cryptography technology in order to protect sensitive communications in real-time environments (King & Hunt, 2000). The Session Layer (5) deals with the creation and control of access to the higher-level applications above, the issue of authorization and access is a natural weakness in this layer. According to Wetteroth (2001), many session layer protocols lack strong protection for their authorization facilities. Protocols such as standard telnet and FTP pass usernames and passwords in the clear, allowing any layer beneath them to intercept their credentials (Rhee, 2003). Rhee (2003) points out that

protocols with stronger protection of passwords such as the Microsoft implementation of CIFS (Common Internet File System, used by MS for file and printer sharing) often fall prey to cryptographic or implementation weaknesses in the handling of passwords and authentication.

Vulnerabilities at this Presentation Layer (6) often originate from weaknesses or shortcomings in the implementation of the presentation layer functions. Gershman (2002) states that continuing on the theme of taking advantage of the original atmosphere of implicit trust and simple functionality that systems were built in, attackers feed unexpected or illegal input into presentation-layer facilities, gaining results that are undesired or contrary to what the original designers intended. Buffer overflows, where program execution can be redirected into completely unintended areas, can be classified at this level as a problem with the presentation of data by an application into the execution environment of the machine (Gershman, 2002). When the presentation from the application exceeds or mismatches the required convention at the presentation layer, unexpected events can happen.

A recently recognized weakness known as format string vulnerability can also be classified in the Presentation Layer (6). Baltatu et. al. (2000) notes that format string vulnerabilities take advantage of applications that use user-supplied information for the basis of input into input-output (I/O) libraries in such a way that the user-supplied data stream could control how that data is transmitted, formatted, or stored in the process of transmission. Henry (2004) points out that this occurs due to either the direct or indirect use of the user input in the format portion of routines used to process the data. Many routines allow this type of use for unformatted, simple output. The assumption is that the user input is passed unformatted and verbatim through the routine. The actual result however, is that the user has access to pass control information through the data channel, and can use this access to crash the program, control its execution, or display arbitrary information on the other end of the output stream (Conorich, 2004).

Controls at the Presentation Layer (6) will typically take the form of cautious and untrusting coding practices when using routines and facilities for network and other inter-process communications. Checking and rechecking input from both the network and the user/application for proper form, and not relying upon lower/upper layers to present properly formed data is a must in an environment thick with arbitrary and deliberately perverse manipulations of communications. Assumptions that ease implementation or time-to-market for systems that shortcut this process may end up being disastrous from a security perspective. User and peer input should always be highly suspect, whether the input is

received from a remote station or a local user (Giese, 2002). Careful specification is needed to determine what is expected from input, and code that carefully checks that input is needed to enforce that specification (Held et al., 2002).

Application Layer (7) security issues include all of the issues discussed so far. However even if a totally secure connection between two systems could be provided, it would not assist in the authentication of a remote user, or in preventing attacks targeted on application layer protocols such as SMTP, FTP or HTTP. Similar to the physical-layer, the open-ended nature of the Application Layer groups many threats together at its end of the stack. According to Tudor (2000), one of the prime threats at the Application Layer (7) is poor or nonexistent security design of the basic function of an application. Some applications may insecurely handle sensitive information by placing it in publicly accessible files or encoding it in hidden areas that are trivially displayed, such as in the HTML code of a web form. Programs may have well-known backdoors or shortcuts that bypass otherwise secure controls and provide unauthorized access (Maiwald, 2002). Applications with weak or no authentication are "prime targets for unauthorized use and abuse over the network" (Heuring et al., 2003, p. 208). The TFTP (Trivial File Transfer Protocol) protocol is extensively used for booting of diskless workstations and network device management, but does not require any sort of username or password authentication to use its file access ability, giving an intruder possible access to configuration and access information without challenge other than the need to guess filenames (Anderson & Schwager, 2002). (This could equally be considered session-layer vulnerability, or the failure to use session-layer controls.) Applications may rely upon untrustworthy channels to establish identity or set privilege.

Some of the most prevalent controls at the Application Layer (7) relate to strong design practices in application design and implementation. Forcht & Ayers (2000) claim that applications should make use of the secure facilities available to them in the lower network layers, carefully check incoming and outgoing data, and assume that communications can and will be subject to attack, requiring the use of strong authentication and encryption to validate and protect data as it travels across the network. Kruh (2002) argues that applications should also implement their own security controls, allowing for fine-grained control of privilege to access resources and data, ideally using a mechanism that is straightforward and strikes a balance between usability and effectiveness. Detailed logging and audit capability should be a standard feature of any application that handles sensitive or valuable data (Kruh, 2002). Testing and review is also critical as a control for the application layer. Given the wide variety of both problems and solutions, standards and practices will not be able to capture all

possible twists and turns in the application environment. Developers will often have conflicting motivations and agendas regarding their applications, and in a structured programming environment, mandated code security review and application security testing are critical parts of a secure Software Development Life Cycle (SDLC).

This section has identified attack risks between the layers of the OSI Model. Similar problems arise with the TCP/IP Model that again was not designed with security as a primary objective. Both network reference models have significant attack risk and make it easy for network communication and for all people to gain entrant to networks. The convenience, however, has come at the cost of security, and the freedom has resulted in an increasing number of attacks on networks. Most of these attacks have been on Operating Systems at the Application layer. However, there has been little attention paid to the security of the physical infrastructure and data link layers, even though malicious attacks can easily be made on these layers.

A review of the fundamental building blocks of networking (the OSI and TCP/IP models) has lead to the following analysis for potential intentional attack types. Some of the important issues that occur in computer network security are present in several layers of both OSI and TCP/IP models (see Table 2.1, Cusack & Sirisukha, 2003).

Table 2.1: Attack risks between OSI and TCP/IP (Cusack & Sirisukha, 2003, p.4)

OSI Layers	**TCP/IP Layers**	**Network Devices**	**Attacks**
7. Application 6. Presentation 5. Session	Application	Gateway	Web-Spoofing (Certificate-Spoofing, SSL-Spoofing) DNS Spoofing; DNS-Cache-Poisoning Message Flooding Distributed Denial of Service (DDOS) HTTP Tunnel, Tunnel RPC (Information gathering)
4. Transport	Transport	Switch	TCP Hijacking; Blind spoofing Denial of Service (DOS)
3. Network	Internet	Router Switch	Route spoofing IP source routing IP source address spoofing
2. Data Link	Host to Network	Switch (Bridge)	ARP-Spoofing (MAC-Address-Spoofing, ARP cache poisoning) MAC Address Table Overload
1. Physical		HUB (Repeater)	Sniffing private Device connecting

2.1.2 Routing Concepts

This section investigates and defines routing protocols for computer networking. It provides an overview of common functions that are shared among various routing protocols. The routing protocols may be categorized as proactive, on-demand, and hybrid, according to the way the computer network exchanges routing information. The concluding subsection then summarises the significant security problems that arise from routing and require further investigation.

Routing is the process of transferring data across an internetwork from a source host to a destination host. Routing can be understood in terms of two processes, host routing and router routing (Bassett, 1998; Tse & Lau, 1998). Host routing occurs when the sending host forwards a packet (IP headers). Based on the destination network address, the sending host must decide whether to forward the packet to the destination or to a router (Tse & Lau, 1998). According to Imielinski & Navas (1999), router routing occurs when a router receives a packet that is to be forwarded. The packet is forwarded between routers (when the destination network is not directly attached to the router) or between a router and the destination host (when the destination network is directly attached) (Richard & Chung, 2000).

According to Kagaris (1997), routers use routing protocols to exchange information regarding routes to a destination. Routing protocols are either unicast (between one sender and one receiver (1-1)) or multicast (between one sender and many receivers (1-M)). A unicast route to a destination is used by a unicast routing protocol to forward unicast data to that destination (Bassett, 1998). A multicast route to a destination is used by some multicast routing protocols to create the information that is used to forward multicast data from hosts on the destination network of the route (known as reverse path forwarding) (Avresky, et al., 1998).

Routing protocols are subject to threats and attacks that can harm individual users or the network operations as a whole (Hardjono & Cain, 1999). The implications for information protection are found in generic threats to routing protocols that include threat sources, threat actions, and threat consequences. The following sub-sections breakdown routing functions in to components and each potential attack identified. This research is a precursor to developing a common set of security requirements for routing protocols. While it is well known that bad, incomplete, or poor implementations of routing protocols may, in themselves, lead to routing problems or failures, or may increase the risk of a network being attacked successfully (Knight, 1998), these issues are not considered here. This study only considers attacks against robust, well-considered implementations of routing protocols.

2.1.2.1 Generic Routing Protocol Threat

Routing protocol attacks can be launched against routing from subverted entities within the routing system and from entities outside the routing system. Both of these types of entities are termed unauthorized entities (Berman, 2000). Routing protocols are subject to threats at the control and data planes and at the functional level. At the control plane level, control and data plane are subject to attack. “An attacker may be able to break a neighbour (e.g., peering,

adjacency) relationship" (Berman et.al., 2000, p. 1093). This type of attack can impact the network routing behaviour in the affected routers and likely the surrounding neighbourhood (Dunsky, 2003) . Foley & Dumigan (2001) note that an attacker who is able to break a database exchange between two routers can also affect routing behaviour. In the routing protocol data plane, an attacker who is able to introduce bogus data can have a strong effect on the behaviour of routing in the neighbourhood (Foley & Dumigan, 2001).

At the routing function level threats can affect the transport subsystem, where the routing protocol can be subject to attacks on its underlying protocol. At the neighbour state maintenance level, there are threats that can lead to attacks that can disrupt the neighbouring relationship with widespread security consequences (Caromel & Vayssiere, 2003). There are threats against the database maintenance functionality. For example, the information in the database must be authentic and authorized. Threats that jeopardize this information can affect the routing functionality in the overall network.

A threat is defined as a motivated, capable adversary. This characterization of threats clearly distinguishes threats form attacks (Scambray et al., 2001; Whitmore, 2001). By modelling the motivations (attack goals) and capabilities of the adversaries who are threats, one can better understand what classes of attacks these threats may mount and thus what types of counter measures will be required to deal with these attacks. A threat is defined as a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm (Shirey, 2000). Whitmore (2001) states that a threat presents itself when an adversary has the ability to take advantage of an existing security weakness. From literature, threats can be categorized based on various rules, such as threat sources, and threat consequences (Berman et al., 2000; Foley & Dumigan, 2001; Householder, Houle, & Dougherty, 2002).

2.1.2.1.1 Threat Sources

There are many sources for threats that may affect routing protocols. In some cases, unauthorized entities such as attackers may illegally participate in the routing operations. In other circumstances, there are threats to routing protocols from entities that are running incorrect code, or using invalid configurations (Cheng & Shen, 1997). Threats can originate form outsiders or insiders. An insider is an authorized participant in the routing protocol. An outsider is any other host or network. A particular router determines if a host is an outsider or an insider. An authorized protocol speaker can be an outsider to a particular router if the

router does not consider it to be a legitimate peer (as could conceivably happen on a multi-access link).

In general, threats can be classified into the following categories based on their sources (Pandey, et al., 2003): (1) Threats that result from subverted links that become subverted when an attacker gains access (or control) to it through a physical medium. The attacker can then take control over the link. This threat can result from the lack (or the use of weak) access control mechanisms as applied to physical mediums or channels. The attacker may eavesdrop, replay, delay, or drop routing messages, or break routing sessions between authorized routers, without participating in the routing exchange. (2) Threats that result from subverted devices (e.g. routers): A subverted device (router) is an authorized router that may have been broken into by an attacker. The attacker can use the subverted device to inappropriately claim authority for some network resources, or violate routing protocols, such as advertising invalid routing information.

2.1.2.1.2 Threat Consequences

A threat consequence is a security violation that results from a threat action (Cotter & Tatham, 1997). The compromise to the behaviour of the routing system can damage a particular network or host or can damage the operation of the network as a whole. There are four types of threat consequences (see description below): disclosure, deception, disruption, and usurpation (Corradi & Stefanelli, 1996).

Disclosure of routing information happens when a router successfully accesses the information without being authorized. Subverted links can cause disclosure, if routing exchanges lack confidentiality. Subverted devices (routers) can cause disclosure, as long as they are successfully involved in the routing exchanges. Although inappropriate disclosure of routing information can pose a security threat or be part of a later, larger, or higher layer attack, confidentiality is not generally a design goal of routing protocols (Cabrera, et al., 2002).

The consequence of deception happens when a legitimate router receives a false routing message and believes it to be true. Subverted links and/or subverted device (routers) can cause this consequence if the receiving router lacks ability to check routing message integrity, routing message origin, and authentication or peer router authentication.

The consequence of disruption occurs when a legitimate router's operation is being interrupted or prevented. Subvert links can cause this by replaying, delaying, or dropping routing messages, or breaking routing sessions between legitimate routers. Subverted devices

(router) can cause this consequence by sending false routing messages, interfering normal routing exchanges, or flooding unnecessary messages. The consequence of usurpation happens when an attacker gains control over a legitimate router's services/functions. Subverted links can cause this by delaying or dropping routing exchanges, or replaying out-dated routing information. Subverted routers can cause this consequence by sending false routing information, interfering routing exchanges, or system integrity.

A threat consequence zone covers the area within which the network operations have been affected by threat actions (Corradi & Stefanelli, 1996). Possible threat consequence zones can be classified as: a single link or router, multiple routers (within a single routing domain), a single routing domain, multiple routing domains, or the global Internet. The threat on sequence zone varies based on the threat action and origin. Similar threat actions that happened at different locations may cause totally different threat consequence zones (Forouzan & Fegan, 2001). For example, when a compromised link breaks the routing session between a distribution router and a stub router, only reach ability to and from the network devices attached on the stub router will be impaired. In other words, the threat consequence zone is a single router. Nonetheless, if the compromised router is located between a customer edge router and its corresponding provider edge router, such an action might cause the whole customer site to lose its connection. In this case, the threat consequence zone might be a single routing domain.

Threat consequence period is defined as a portion of time during which the network operations have been impacted by the threat consequences (Simon, 2003). The threat consequence period is influenced by, but not totally dependent on the duration of the threat action. In some cases, the network operations will get back to normal as soon as the threat action has been stopped. In other cases, however, threat consequences may appear longer than threat action. For example, in the original ARPANET link-state algorithm, some errors in a router might introduce three instances of an LSA, and all of them would be flooded throughout the network forever, until the entire network was power cycled (Flammini et.al., 1998).

2.1.2.2 Multicasting Routing

Multicasting is a network service that provides many-to-many communication (Hee et.al., 2003; Kodialam et.al., 2003). It uses the notion of a group of members associated with a given group address (Chen et.al., 2002). A sender simply sends a message to this group address and the network replicates the message at suitable junctions and forwards the copies

to group member located throughout the network (Jeong et.al., 2002). Feng et.al., (2002) suggest that in order to achieve this convenient replication effect the router in the network must maintain some state or information regarding a given multicast group. The maintenance of this state is achieved using a multicasting routing protocol, which creates a logical distribution tree. Examples of multicast routing protocols are Distance Vector Multicast Routing Protocol (DVMRP), Multicast Open Shortest Path First (MOSPF), Core Based Tree (CBT), Protocol Independent Multicasting-Dense Mode (PIM-DM) and Protocol Independent Multicasting-Sparse Mode (PIM-SM) (Ballardie et.al., 1993; Moy, 1994; Pusateri, 1998).

In the multicast model, Sarkar & Tassiulas (2002) state that a host joins a group by using the Internet Group Management Protocol (IGMP) that runs between a host and the subnet-routers. IGMP allows the host to indicate to the subnet-router that it wishes to receive packets destined for a given multicast group address (Lin & Lai, 2000). Here, the subnet-router is interested only in whether or not there is receiver for given multicast group. It does not maintain information about the membership of any given group (Gunes et.al., 2001). Thus, the subnet-router is only concerned about the active groups in its subnet. The security risk lies in the multicast model that allows the receivers to remain anonymous. The subnet routers do not propagate any identification information to the other members of the group (Lin & Lai, 2000). Yang & Park (2001) point out that IP multicast must be efficient, scale well and be incrementally deployable. Samadian-Barzoki et.al. (2004) have noted that it is the setting up and maintaining of the group that is to require to minimise control messages. Li et.al. (2003) point out that the number of control messages and the amount of state in network elements should grow linearly with the number of receivers and the size of the network. By incrementally deployable, Han & Yang (2003) define that it is meant that it should be possible to add the multicast algorithm to the Internet without requiring a simultaneous change to all routers and endpoints.

The Internet Engineering Task Force (IETF) recommended standard, RFC 1112, define extensions to the Internet Protocol (IP) (Pandey et al., 2003). A relatively new feature of the IP, IP multicast is a protocol for transmitting IP datagrams from one source to many destinations in a LAN or WAN. Groups of receivers participate in multicast sessions. With IP multicast, applications send one copy of the information to a group address. The information reaches all the recipients who want to receive it. Multicast technology addresses packets to a group of receivers rather than to a single receiver; it depends on the network to forward the packets to only the networks that need to receive them. Multicast-enabled nodes that run the TCP/IP suite of protocols can receive multicast messages (Chen et.al., 2000). Multicasting is

using push and pull technology (Filali & Dabbous, 2002). The terms push and pull appear frequently in discussion of how information is delivered over the Internet. In push technology server sends data to a client without the client requesting it. On another hand, pull technology a client requests data from a server or from another computer. Email is examples of push technology while the web is based on pull technology (Gunes et al., 2001). In this case the client browser requests the delivery of a page. Standards-based IP multicasting supports thousands of users simultaneously without substantially effecting bandwidth requirements (Hardjono & Cain, 1999). In addition, IP multicast routing protocols provide efficient delivery of datagrams from one source to any number of destinations throughout a large, heterogeneous network such as the Internet. If the network hardware supports multicast, then a packet destined for multiple recipients can be sent as a single packet.

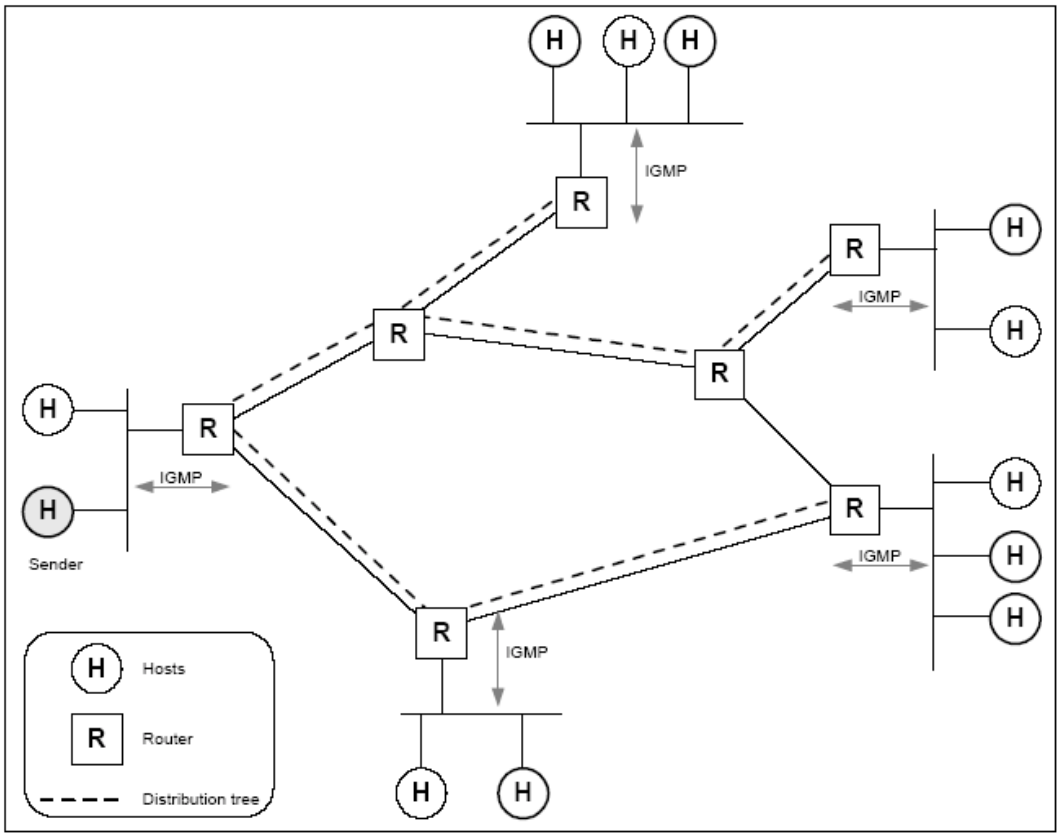

Figure 2.3 Operation of IP Multicasting (Hardjono & Cain, 1999, p. 27)

Figure 2.3 shows a simplified depiction of the basic IP multicasting model. IGMP is running in the subnet-routers (R) with attached hosts (H), and only one group is in existence (Hardjono & Cain, 1999). The members of the group are depicted as circles with thicker

lines. The dashed-lines indicate the path of traversal of the packets of the multicast group, from the sender to the receivers (hosts) in the various subnets. Alvarez-Hamelin & Fraigniaud (2003) claim that the IP multicast model is attractive because it can scale to a large numbers, subject only to the resources available to the underlying multicast routing protocol. However, Wan et.al., (2003, p. 68) state that this scalability is achievable precisely because of the "anonymous-receiver" behaviour inherent in the model, as expressed through IGMP. In order words, scalability is achieved due the fact that no host-identification information is maintained by the routers (Chen & Singh, 2002). Any host in subnet can join a multicast group without its subnet router passing identification information about the host to other routers upstream in the distribution tree (Ravindran & Liu, 2002).

2.1.2.3 IPv4 Multicast Addressing

Changes have occurred to the definition of network as the protocol definition has changed. This section starts with a description of what IPv4 is before going on to outline the global IPv4 address environment and how the global address space is managed through regional registries and organizations such as Internet service providers (IPSs) for distribution to end users. This is followed by an examination of the process for obtaining addresses for an end user, which highlights some of the rules, which have to be followed by the ISP as apart of this process. Chen & Singh (2002) point out that the penalties for abuse of this system are punitive and could seriously affect the ability of an ISP to conduct its business.

Internet Protocol Version 4 (IPv4) addresses are made of up four 8-bit fields (octets) and are 32-bits in size total (Lund et.al., 1999). IPv4 address is "invisibly divide into two parts, the first part identifies a particular network, and the second part identifies a particular machine on that network which is called host" (Bouras et.al., 2003, p. 86). The point at which the first part, the network part, of the address ends and the second part, the host part, of the address begin depends upon the size of the network. Yoke (2002) suggests that if the network is very large, with many hosts, the division point is nearer the beginning of the address that it would be in a smaller network with fewer hosts. For instance, with the address 132.146.100.100, the first two numbers (132.146) may refer to a single large network, leaving address space from 0.0 through to 255.255 (i.e. approximately 65000 addresses). Whereas the address 194.72.10.10 may be the address of host on a smaller network represented by the numbers 194.72.10, which leave only 255 addresses on that network (0 to 255).

FitzGerald & Dennis (2002) mention that the exact position of this division point is denoted by the subnet mask, which indicates which part of the address represents the network, and which represents the host. The 132.146.100.100 address would have a subnet mask of '255.255.0.0', the 255s indicating which numbers represent network, and the zeros indicating which numbers represent the hosts on that network, the 194.72.10.10 example would have the subnet mask '255.255.255.0'. What is in fact happening here is that every bit in the 32 bits of the address that represents the network is being masked with a '1', and every bit that represents a host is being masked with a zero. Thus the subnet mask for the first example is actually 11111111. 11111111.00000000. 00000000, but for convenience this is converted to decimal and written as 255.255.0.0.

Panko (2000) states that the first address on a network cannot be given to a host on network, since it is used to represent the network as a whole. For example by the address 194.72.10.0, with a subnet mask of 255.255.255.0 is the first address on that network, and is used only to represent that entire network (Tanenbaum, 2002). This is called a network address. Similarly the last address on a network cannot be given to the host, since this is used as broadcast address. Any traffic sent to a broadcast address is effectively addressed to all the hosts on that network. The address 194.72.10.255 with subnet mask 255.255.255.0 is a broadcast address (Tanenbaum, 2002).

According to Black (2000), IPv4 organizes the networked world into a two-level hierarchy: network numbers, and host numbers within network numbers. Currently the Internet Assigned Numbers Authority (IANA) largely delegates to Internet service providers the job of assigning unique network numbers to organizations that request them (Forouzan et. al., 2001). The organization's network administrator then assigns unique host numbers to its attached devices. King & Hunt (2000) point out that IPv 4 supports the standard classes of address, which defines which bits are used for the network ID and which bits are used for the host ID.

In an IPv4 implementation, each physical network and host has its own unique network address. Routers or gateways can have one or more addresses depending on the number of interfaces present. There are three fundamental types of IPv4 addresses: unicast, broadcast, and multicast (Mark Pullen, 2000). The unicast address transmits a packet to a single destination IPv4 recognizes three kind of unicast addresses classes, A, B, C, that identify a specific network interface addresses (Ohata et al., 2001). A broadcast address sends a datagram to an entire subnetwork. A multicast address enables the delivery of datagrams to

a set of hosts configured as members of a multicast group in various scattered subnetworks. A class D address is a multicast address.

The IPv4 address space is divided into classes consisting of three kinds of unicast addressed (Johnston, 1998), A, B, and C, that identify a specific network interface addresses. A unicast address identifies a specific network interface addresses. Class A addresses are intended for use by the world's largest organizations while class C addresses are intended for very small network communities. An existing pool of class C addresses supports the current growth in the Internet. More (but still not that many) organizations would support between 256 and 65,534 hosts that a Class B network allows. IPv4 also two specialized address classes: D and E. Rather than being assigned to specific interface, a Class D address identifies the members of logical group of interfaces. All logical holders of a particular Class D address receive packets sent to that address. Classless Inter-Domain Routing is making the IP address classes in their current form less defined (Ferraris et.al., 2001). Still, the classes form the base of any addressing scheme. The Internet Assigned Numbers Authority (IANA) reserves Class E addresses for future and experimental uses.

IPv4 addresses are made of both a network ID and a host ID. The network ID address identifies the physical network where the hosts exist. The host ID address identifies the individual TCP/IP host on a network. The host ID must be unique on the internal network; that is, no two nodes on a given network can have the same network ID and host ID.

2.1.2.4 IPv6 Multicast Addressing

A new protocol has been adopted to upgrade and improve the network capacities of IPv4. This section presents an overview and discusses the current Internet IPv4 issue of security and privacy problems. The Next Generation Internet Protocol (IPng) or IPv6 is designed to redress some of these shortcomings and these capacities are elaborated. IPng was recommended by the IPng Area Directors of the Internet Engineering Task Force at the Toronto IETF meeting on July 25, 1994, and documented in RFC 1752, "The Recommendation for the IP Next Generation Protocol" (Nicolle, 2001, p. 44) . The recommendation was approved by the Internet Engineering Steering Group on November 17, 1994 and made a Proposed Standard (Wieland, 2002). The formal name of this protocol is IPv6 (where the "6" refers to it being assigned version number 6) (Mackay et.al., 2003).

IPng solves the Internet scaling problem, provides a flexible transition mechanism for the current Internet, and was designed to meet the needs of new markets such as nomadic personal computing devices, networked entertainment, and device control. It IPv6 includes an

improved option mechanism over IPv4. IPv6 options are placed in separate extension headers that are located between the IPv6 header and the transport-layer header in packet. Most IPv6 extension headers are not examined or processed by any router along a packet's delivery path until the packet arrives at its final destination. This facilitates a major improvement in router performance for packets containing options. In IPv4 the presence of any options requires the router to examine all options. The other improvement is that, unlike IPv4 options, IPv6 extension headers can be of arbitrary length and the total amount of options carried in packet is not limited to 40 bytes. An example of this is the IPv6 Authentication and Security Encapsulation process.

IPv6 increases the IP address size from 32 bits to 128 bits, to support more levels of addressing hierarchy and a much greater number of addressable nodes, and simpler auto-configuration of addresses (Simco, 2001). This has implications for better security. There are three types of addresses as following unicast, anycast, and multicast (Grosse et.al., 2003). Unicast is to identify for a single interface. A packet sent to a unicast address is delivered to the interface identified by that address. Anycast is to identify for a set of interfaces (typically belonging to different nodes). A packet sent to an anycast address is delivered to one of the interfaces identified by that address (the nearest one, according to the routing protocols' measure of distance). Multicast is to identify for a set of interfaces (typically belonging to different nodes). A packet sent to a multicast address is delivered to all interfaces identified by that address. There are no broadcast addresses in IPv6, their function being superseded by multicast addresses.

The current Internet has number of security problems and lack effective privacy and authentication mechanisms below the application layer. IPv6 remedies these shortcomings by having two integrated options that provide security service. These two options may be used singly or together to provide differing levels of security to different users. This is critical because different user communities have different security needs. The first mechanism, called the IPv6 Authentication Header, is an extension header that provides authentication and integrity (without confidentiality) to IPv6 datagrams. While the extension is algorithm-independent and will support many different authentication techniques, the use of keyed MD5 is required to help ensure interoperablity within the worldwide Internet (MD5 is algorithms for computing a condensed representation' of a message or a data file.). This can be used to eliminate a significant class of network attack, including host masquerading attacks. The use of the IPv6 Authentication Header is particularly important when source routing is used with IPv6 because of the known risks in IP source routing. Its placement at

the Internet layer can help provide host origin authentication to those upper layer protocols and services that currently lack meaningful protections. This mechanism should be exportable by vendors in the U.S. and other countries with similar export restrictions because it only provides authentication and integrity, and specifically does not provide confidentiality. The exportability of the IPv6 Authentication Header encourages its widespread deployment and use.

The second security extension header provide with IPv6 is the IPv6 Encapsulating Security header. This mechanism provides integrity and confidentiality to IPv6 datagrams. It is simpler than some similar security protocols but remains flexible and algorithm-independent. To achieve interoperability within the global Internet, the use of Data Encryption Standard (DES) - Cipher Block Chaining (CBC) is being used as the standard algorithm for use with the IPv6 Encapsulating Security Header. Some IPv4 header fields have been dropped or made optional, to reduce the common-case processing cost of packet handling and to keep the bandwidth cost of the IPv6 header as low as possible despite the increased size of the addresses (Kijkanjanarat & Chao, 1999). Even though the IP6 addresses are four times longer than the IPv4 addresses, the IP6 header is only twice the size of the IPv4 header.

IPv6 includes an improved security option mechanism over IPv4. IPv6 options are placed in separate extension headers that are located between the IP6 header and the transport-layer header in a packet (Gyires, 2003). Most IPv6 extension headers are not examined or processed by any router along a packet's delivery path until it arrives at its final destination (Lawson, 2003). This facilitates a major improvement in router performance protection for packets containing options. In IPv4 the presence of any options requires the router to examine all options. The other improvement is that unlike IPv4 options, IP6 extension headers can be of arbitrary length and the total amount of options carried in a packet is not limited to 40 bytes (Wieland, 2002). This feature plus the manner in which they are processed, permits IPv6 options to be used for functions, which were not practical in IPv4. An example of this is the IPv6 Authentication and Security Encapsulation options (Dabbous, 1997).

2.1.2.5 Multicasting Security Concerns

While multicast routing provides an efficient many-to-many service, it does not limit or control what can use the service. Any host can send to a multicast group or elect to receive the traffic from that group. Because of this, most of the efforts to provide a secure multicast

service have focused on providing mechanisms for distributing encryption keys to those participants authorized to have them, for authenticating messages, and re-keying the group as required when members join or leave. The first efforts to provide secure multicast were unscaleable, because either they required a single server to compute the key for a group, or they required extensive knowledge about the group membership (Hee et. al., 2003). Distributed and scalable methods of keying a multicast group have also been proposed (Im & Choi, 1998). In these protocols, the encrypted data are still available to any interested receiver, and in the case of flood and prune protocols, will actually be sent to all possible receivers, unless they prune themselves from the tree (Kodialam et. al., 2003).

Providing security for complete multicast services, while viable, is inefficient and vulnerable to attacks against the encryption being used (Lin & Lai, 2000), because every interested attacker can have access to the data. While it may be possible to use stronger encryption to help thwart an attack, the approach may be limited by the political and legal policies regarding the use of encryption. Additionally, an attacker may be able to gain useful information without breaking the encryption by using traffic analysis (Motyckova & Jennings, 1999). Multicasting also provides an efficient means for a denial-of-service attack, through which an attacker can send large amounts of data to the multicast address being attacked. This data is copied and sent to all receivers, possibly creating congestion in the network that prevents legitimate users from being able to participate in the group.

It is therefore desirable to limit participation in a secure multicast group to only those group members authorized to participate. Pan et. al. (2003) pointed out the need for some type of authentication and authorization mechanism for multicast. They also clearly stated the goals that a secure multicast protocol design should meet: compatibility with existing protocols, scalability to the scope of the global Internet, transparency to higher-level protocols, localizability for gradual introduction of the technology and flexibility to support a variety of policies (p. 14). However, the authors did not create any protocol meeting these criteria.

The first attempt to provide for authentication and authorization in an existing multicast routing protocol came in some simple extensions to CBT (CBT is a multicast routing architecture that builds a single delivery tree per group which is shared by all of the group's senders and receivers) that attempted to regulate access to the multicast tree at the first hop router (Sarkar & Tassiulas, 2002). Wang et.al. (2002) explained that the need for Secure IGMP (Internet Group Management Protocol) is the protocol that hosts users to communicate with an attached router and initiate its connection with the multicast group

(Zhang et.al., 2001), which could present cryptographic credentials from the host to the router. However, their protocols did not meet secure design requirements. To begin with, there was no mechanism for key distribution, and since all authorization was done at the leaf router on the tree, a corrupt router compromised the entire scheme. Additionally, rather than preventing flooding attacks, the protocol attempted to detect and squelch such attacks by randomly sampling packets and, upon detection of unauthorized traffic, sending messages towards the putative source that prevented it from forwarding traffic onto the tree. The problem with this scheme is that it leads to a simple and effective denial of service attack. An attacker, in conjunction with one corrupt router, could send unauthorized traffic that was forged with the source address of the target of the attack. When these packets were detected, the innocent target would be removed from the tree, and expose the victim of the forgers (Yoon et al., 2002).

Xianwei et.al. (2000) examined the problems inherent in maintaining the efficiency of multicast routing while providing a secure service. This work introduced four methods of reducing the size and number of control messages needed to authenticate group members and to distribute encryptions keys to the group. First, they pointed out that a multicast tree consisted of branches, each of which could utilize different control information than other branches. A node on the tree could then tailor messages for each branch separately, rather than send information needed by only one branch to all branches. Second, they showed that an intermediate node could do some message re-processing, including re-arranging or re-encrypting the message so long as the message's integrity and origin were maintained. This is significant, because it means that a sender does not need to know the topology or group membership to trim control branches, at the bottom of which the messages are reprocessed for sub-branches. Xianwei et. al. (2000) also pointed out that shared tree protocols are ideal for this type of re-processing, because protocols that have distributed cores can use them as natural spots for message re-processing, in effect breaking one at tree down into a hierarchy of smaller trees, each of which has its own control traffic. Third, they pointed out that group re-keying need not take place only at the time a member joins or leaves the group, but can be pre-computed; they call this hot start authentication. Finally, they extend the idea of hot start authentication to continuous authentication, under which each member needs to periodically re-authenticate to receive the current key. These four security ideas re-occur in later works in the area.

2.2 VIRTUAL PRIVATE NETWORKS (VPNs)

A key element for protecting information in a BIS is the Virtual Private Network (VPN). The VPN provides businesses with an economical means by which to communicate information securely over public networks. It is both cost efficient and context effective for businesses. According to Pena & Evans (2000), VPN can be formally defined as a communication environment constructed by controlled segmentation of a shared communication infrastructure to emulate the characteristics of a private network. The access to the communication environment is controlled to permit interconnections for a defined community; even though, the underlying shared communications infrastructure provides services on a non-exclusive basis. VPN is a network that provides inter-connectivity to exchange information among various entities that belong to the VPN (Al-Khayatt et.al., 2002). A BIS is also given flexibility for "the mobility of today's workforce" (Patton et.al., 2000b, p. 225) with VPN use. Many organizations are increasing employee's productivity by equipping them with portable computing facilities. Affordable laptops and various palm-based devices have made it easy for people to work without being physically present in their offices. Besides potential increased productivity, organizations are encouraging telecommuting to reduce their investments in real estate, commuter time, and environmental pollution from automobiles (Broadhead, 2000).

A private network supports a closed community of authorized users, allowing them to access various network related services and resources (Gengler, 1999). The traffic originating and terminating within a private network traverses only those nodes that belong to the private network. Further, there is traffic isolation. That is, the traffic corresponding to this private network does not affect nor is it affected by other traffic extraneous to the private network. A VPN creates a private network virtually on public networks. McGregor & Lee (2000) point out that the main reason that organizations use VPN security is so that they can transmit sensitive information over the Internet without needing to worry about who might see it. Everything that goes over a secure VPN is encrypted and packaged (tunneled) to such a level that even if someone captured a copy of the traffic, they could not read the traffic. Further, using a secure VPN allows the organization to know that an attacker cannot alter the contents of their transmissions, such as by changing the value of financial transactions (Zhang & Zheng, 2001). The term shared network infrastructure has been used to describe the underlying infrastructure on which the VPN is constructed (Antonopoulou et al., 2001). This can either be the public Internet or network consisting of one or more service providers.

A Virtual Private Network (VPN) can help resolve many of the issues associated with network security. Global VPN enable connectivity to all locations anywhere in the world at a fraction of the cost of dedicated links. Two popular tunneling protocols are the Point-to-Point Tunneling Protocol (PPTP) and Internet Protocol Security (IPSec). The benefit of using PPTP is that it is built into the Windows operating system allowing any client running Windows to securely connect to the corporate VPN gateway. IPSec, on the other hand, requires client software for remote users. IPSec's advantage is that it provides better overall security with stronger encryption, and higher performance than PPTP. VPN services enable remote access to the Intranet at significantly lower cost, thus enabling support for a mobile workforce. Additionally, the VPN architecture supports a reliable authentication mechanism to provide easy access to the Intranet from anywhere using any available access media including analog modems, Integrated Services Digital Network (ISDN), cable modems, Digital Subscriber Line (DSL) and wireless. There are three types of VPN services (He, Blight, & Chujo, 2000); Interconnect VPN services, Dial-up VPN services, Extranet VPN services. The following sections define various VPN prpoerties and services.

2.2.1 Interconnect Services

He et al. (2000a) defined Interconnect VPN services as help to interconnect local area networks located at multiple geographic areas over the shared network infrastructure. Typically, this service is used to connect multiple geographic locations of a single company. Several small offices can be connected with their regional and main offices and expensive dedicated links replaced. The capacity of any of the links depending on the applications supported on the VPN can easily be increased. As applications change with time, the architecture can be adapted to meet the needs. Further, additional geographical sites can be connected to the VPN with very little effort.

2.2.2 Remote Access VPN Services

The Dial-up VPN service supports mobile and telecommuting employees in accessing the organization's Intranet from remote locations (Schafer, 2001). The remote employee (user) dials into the nearest Remote Access Server (RAS, the technical term for modem pool). This is typically a local Point-of-Presence (PoP) of an Internet Service Provider (ISP) or the shared network infrastructure. In one dial-up VPN model, called the Layer 2 Tunneling Protocol (L2TP), the RAS automatically establishes a secure connection to a pre-specified location inside the organization's Intranet, usually through a firewall enhanced with VPN

capabilities (Cui & Bassiouni, 2003). Contingent upon successful authentication of the user, the secure connection enables the user to transparently connect to the Intranet. The L2TP model is also known as a static VPN connection and is usually aimed at home offices and telecommuters who dial-in to a specific local RAS.

2.2.3 Extranet VPN Services

An extranet VPN service combines the architecture of Interconnect VPN services and dial-in VPN services (Box & Sterling, 2001). This infrastructure enables external vendors, suppliers and customers to access specific areas of the organization's Intranet. The allowed specific area is denoted as the Demilitarized Zone (DMZ) (Claxton, 2001). When a supplier's representative connects to the organization's Intranet, either from the supplier's Intranet or dialing in remotely, the firewall and authentication mechanisms ensures that the connection is directed to the DMZ. A company employee (user), on the other hand, has full access to the organization's Intranet. The flexibility of the extranet services helps to provide connectivity to new external suppliers and customers within a short period of time (Schafer, 2001). The fast communications facilitated by the extranet helps in several e-commerce areas including efficient inventory management and electronic data interchange (EDI). This provides significant savings in cost and the ability to effectively compete in the rapidly growing market.

2.2.4 Buiness VPN

Businesses work with both public and private networks. Private networks can be achieved by either setting up LANs or by using VPN software. A BIS can consequently be a LAN (VAN etc), a VPN or a combination of each. The subsequent definition of the BIS has direct consequences for the business capability. A LAN for example limits secure business activity to one location. However, with addition of VPN to the LAN (or in VPN in isolation) a business can now securely transact information across greater distances. A VPN restricts traffic to exchange between specified sites both directions – send and receive. A cost benefit is gained from VPN implementation by businesses as they can use both private and public networks securely and without having to enter into the costly expense of building their own wide area networks (Wan, et al., 2001). To achieve WAN capacity through VPN a business only has to connect two networks over an intranet using a router-to-router VPN connection. This type of VPN connection might be necessary, for example, for two departments in separate locations, whose data is highly sensitive, to communicate with each other. For

instance, the finance department might need to communicate with the human resources department to exchange payroll information. The finance department and the human resources department are connected to the common intranet with computers that can act as VPN clients or VPN servers. Once the VPN connection is established, users on computers on either network can exchange sensitive data across the corporate intranet.

2.2.5 IP Security (IPSec)

IP Packets have no inherent security. It is relatively easy to forge the addresses of IP packets, modify the contents of IP packets, replay old packets, and inspect the contents of IP packets in transit. Therefore, there is no guarantee that IP datagrams received are (1) from the claimed sender (the source address in the IP header); (2) that they contain the original data that the sender placed in them; or (3) that the original data was not inspected by a third party while the packet was being sent from source to destination (Cheung & Misic, 2002). IPsec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services. IPsec can be used to protect one or more paths between a pair of hosts, between a pair of security gateways, or between a security gateway and a host (Aqun, et al., 2000). (The term security gateway is used throughout the IPsec section to refer to intermediate systems that implement IPsec protocols. For example, a router or a firewall implementing IPsec is a security gateway.)

2.2.5.1 The Architecture

IPsec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6 (McLoone & McCanny, 2002). The set of security services offered includes access control, connectionless integrity, data origin authentication, protection against replays (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow Confidentiality (Box & Sterling, 2001). These services are provided at the IP layer, offering protection for IP and/or upper layer protocols.

These objectives are met through the use of two traffic security protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP) (AH and ESP explain more detail in sections 7.2 and 7.3), and through the use of cryptographic key management procedures and protocols (Harding, 2003). The set of IPsec protocols employed in any context, and the ways in which they are employed, will be determined by the security and system requirements of users, applications, and/or organizations.

When these mechanisms are correctly implemented and deployed, they ought not to adversely affect users, hosts, and other Internet components that do not employ these security mechanisms for protection of their traffic (Raz & Shavitt, 2000). These mechanisms also are designed to be algorithm-independent. This modularity permits selection of different sets of algorithms without affecting the other parts of the implementation. For example, different user communities may select different sets of algorithms (creating cliques) if required. A standard set of default algorithms is specified to facilitate interoperability in the global Internet (Redlich, et al., 1999). The use of these algorithms, in conjunction with IPsec traffic protection and key management protocols, is intended to permit system and application developers to deploy high quality, Internet layer, cryptographic security technology.

2.2.5.2 The Authentication Header (AH)

The AH protocol can detect packet corruption or tampering and can authenticate the identity of a sender by end user or by source IP address. Currently, the IPsec peers (communicating parties) in AH may use either MD5 or SHA-1 (MD5 and SHA1 are algorithms for computing a condensed representation of a message or a data file.) to create a hash signature using a secret component of the SA, the packet data payload, and several parts of the packet header (Marsan, 2001a). Figure 2.4 shows a typical authentication header (Davies & Lee, 1999). The AH header has five essential fields: The next header, which usually describes the layer 4 header (TCP/UDP/ICMP) for an IPv4 datagram; The length of the hash signature (note that this value will be constant for each hashing algorithm, since each has a fixed-length output); The security parameter index (SPI); The anti-replay sequence number field (this prevents an attacker from *replaying* [resending] a packet as part of an attack); and, The hash signature itself.

To transmit an AH packet, the IPsec host or gateway must do the following: Identify the appropriate SA, SPI, algorithm (MD5 or SHA-1), and secret key; Increment the anti-replay counter (anti-replay is on by default); Assemble the data to be hashed in a fashion appropriate to the specific standard in force; Set the time to live (TTL), type of service (ToS, now known as the differentiated services or DS byte), and header checksum fields to zero.

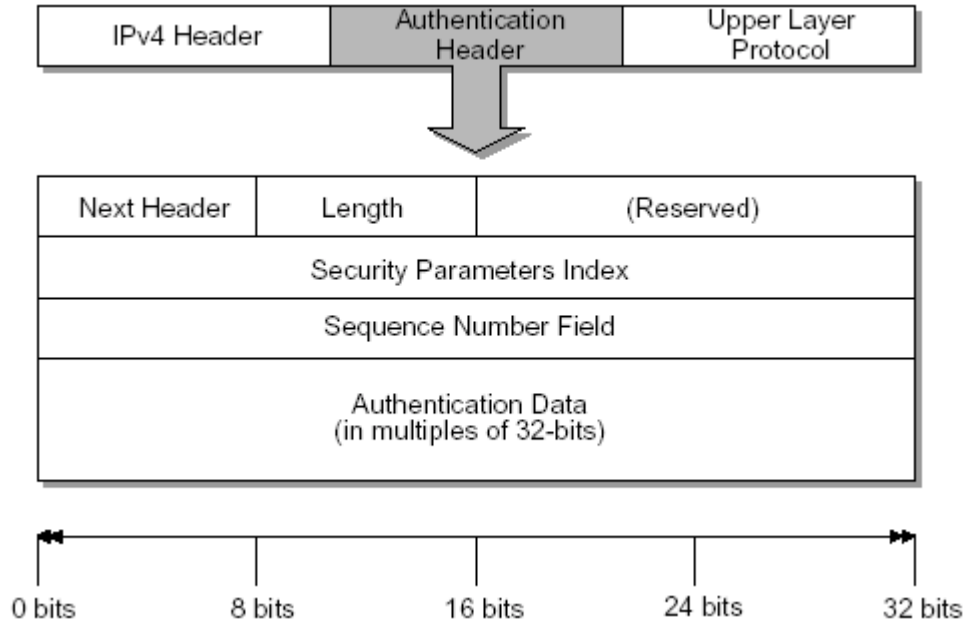

Figure 2.4 A typical authentication header (AH) adopted from Davies & Lee (1999, p. 61)

This operation allows these fields to be modified in flight without altering the hash signature. (Note that for IPv6, you also need to zero out the hop limit field in the base header and all fields whose OPTION TYPE bit is set to indicate a mutable value.); and, Calculate the hash value and the other packet header fields. Also insert the AH header directly between the IP header and the layer 4 header. In tunnel mode, the entire original datagram is the packet payload, so the AH header goes between the newly created outer IP header and the original datagram. (Note that for IPv6, the AH header belongs after all hop-by-hop headers.)

A receiving (see figure 2.4) host or gateway reverses the transmission process described in the previous section and discards any datagrams whose recalculated hash value doesn't match the original. If the relevant SA specifies anti-replay, the sequence number must fall within the proper window (range) of numbers, and must not be a duplicate of any prior packet. Figure 2.5 shows detail of an authentication header (Davies & Lee, 1999).

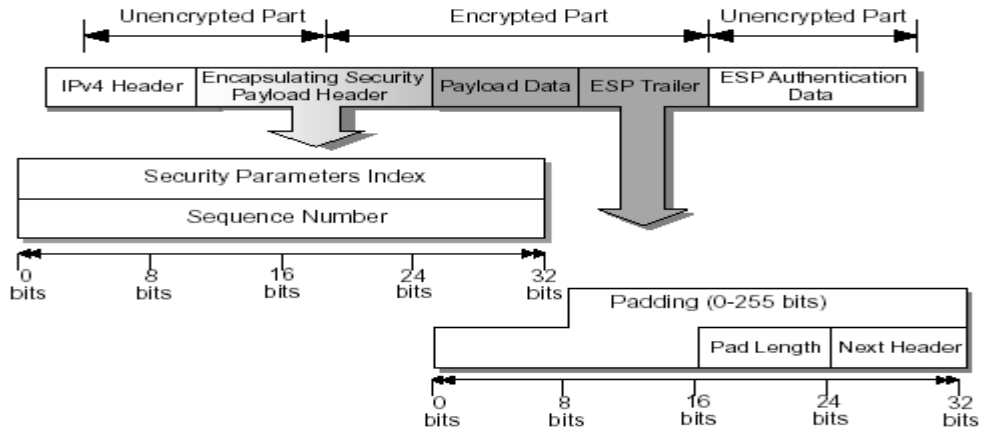

Figure 2.5 Authentication header (AH) detail (Adopted from Davies & Lee (1999, p. 67).

2.2.5.3 The Encapsulating Security Payload (ESP)

The ESP protocol can provide confidentiality, authenticity, and integrity services. Tunnel-mode ESP also offers traffic-flow confidentiality. Early drafts of the ESP protocol focused on confidentiality, but the final standard also includes functionality from AH (Braun, et al., 2001). The ESP standards currently support two transforms, or operations: DES (Data Encryption Standard) and 3DES (El-Sayed & Jaffe, 2002). The two transforms are very similar, and DES support is mandatory. The ESP standard will eventually support transforms for many other encryption algorithms. Like AH, the ESP header contains (Maresca, et al., 2002) the security parameter index (SPI) and the anti-replay sequence number field. Unlike AH, the ESP header also includes the next header field as part of the packet trailer. The packet payload may include padding to conform to the specific cryptographic transform and to ensure that the next header field ends on a 4-byte boundary (Kuo & Burns, 2000). The trailer may also contain a variable amount of authentication data.

A receiving host or gateway reverses the sending procedure described in the previous section. If the SA specifies authentication services, that check essentially mirrors the hash check for AH: The host or gateway must discard any packet that fails the integrity check. If the SA specifies the anti-replay option, the host or gateway must also discard any packets that are repeats or that fall outside the receiver's window. The last step is to decrypt the packet payload (Baek, et al., 2000). Figure 2.6 shows an ESP-transformed datagram (Davies & Lee, 1999). In this example the datagram contains an optional ICV that provides authenticity and integrity. If the ICV were not present, IPsec would not detect modification to the payload, but the decryption would probably produce gibberish. An ICV generally provides a more positive mechanism for discarding modified data with minimal overhead.

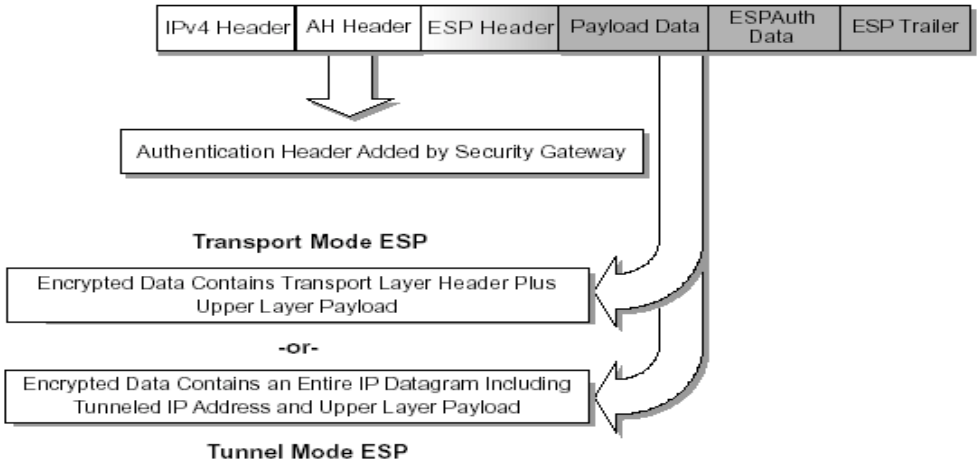

Figure 2.6 AH and ESP headers together adopted from Davies & Lee (1999, p. 72)

2.2.5.4 Authentication Header (AH) & Encapsulating Security Payload (ESP)

AH and ESP can operate on the same datagram. Although it is possible for an end host or gateway to apply both protocols to the same connection, that scenario is not the most common. In a more typical combination, the end host generates transport-mode ESP datagrams, while an intermediate security gateway (SG) encapsulates those ESP packets into tunnel-mode AH (Labonte & Srinivas, 2000). A mirror-image configuration at the other end of the connection (an SG de-encapsulates, and an end host decrypts) would provide end-to-end confidentiality and a strong defense against tampering across the WAN. The inverse configuration—in which the end host uses AH and the gateway tunnels ESP—would also make sense for many VPN topologies.

2.2.5.5 Encryption

Encryption is optional in a VPN. As an optional component it has the capacity to add another layer of protection to information transfer and in practice it is used in three ways. One to encrypt the initial negotiations as the tunnel is set up. Second for client access to the tunnel, and thirdly for messages being sent through the tunnel. The VPN tunnel is created independently of the encrypting of the messages to be sent to and through the tunnel and each use of encryption can be independent. As a consequence a message may be encrypted or not (Lierley, 2002). Different protocol use different algorithms to encrypt. For example, when the IPSec tunnel is set up the process uses Diffie-Hellman encryption for negotiations. The PPTP protocol bases encryption on the RSA/RC4 algorithm. Similarly the use of keys and their management varies between protocols so that for example, the L2TP protocol uses IPSec security that negotiates a common key during the ISAKMP exchange. The PPTP protocol uses an initial key generated during user authentication and both protocols rely on periodic refreshing of keys for protection (Lee & Davies, 2000). Encryption is one further layer of protection that is available in the complex set of VPN securities.

2.2.6 Point-To-Point Tunnelling Protocol (PPTP)

The PPTP protocol is built on the well-established Internet Communications Protocol PPP (point-to-point protocol), and TCP/IP (Transmission Control Protocol/Internet Protocol) (FitzGerald et al., 2000). Multiprotocol PPP offers authentication as well as methods of privacy and compression of data. IP (Internet Protocol) is routable, and has an Internet

infrastructure. PPTP allows a PPP session to be tunneled through an existing IP connection, no matter how it was set up. An existing connection can be treated as if it were a telephone line, so a private network can run over a public one.

Tunneling is achieved because PPTP provides encapsulation by wrapping packets of information within IP packets for transmission through the Internet (Yuan, et al., 1998). Upon receipt, the external IP packets are stripped away, exposing the original packets for delivery. Encapsulation allows the transport of packets that will not otherwise conform to Internet addressing standards (Harding, 2003). PPTP encapsulates Point-To-Point Protocol (PPP) frames into IP data grams for transmission over an IP-based Internet work, such as Internet (Zhang & Zheng, 2001). To encapsulate PPP frames as tunneled data, PPTP uses a TCP connection known as PPTP control connection to create, maintain and terminate the tunnel & a modified version of Generic Routing Encapsulation (GRE) (Gentry, 2001).

2.2.6.1 Tunnel Maintenance with the PPTP Control Connection

The PPTP control connection is between the IP address of the PPTP client using a dynamically allocated TCP port and the IP address of the PPTP server using the reserved TCP port 1723 (FitzGerald, 2002). The PPTP control connection carries the PPTP call control and management messages that are used to maintain the PPTP tunnel. This includes the transmission of periodic PPTP Echo-Request and PPTP Echo-Reply messages to detect a connectivity failure between the PPTP client and PPTP server. PPTP control connection packets consist of an IP header, a TCP header, and a PPTP control message. The PPTP control connection packet in Figure 2.7 also includes a data-link layer header and trailer (Yuan et al., 1998).

Data - Link Header	IP	TCP	PPTP Control Message	Data - Link Trailer

Figure 2.7 PPTP Control Connection Packets adopted from Yuan et al. (1998, p. 129)

2.2.6.2 Encapsulation of PPP Frame

The initial PPP payload is encrypted and encapsulated with a PPP header to create a PPP frame. The PPP frame is then encapsulated with a modified Generic Routing Encapsulation (GRE) header. GRE is documented in RFC 1701 and RFC 1702 (Hanks, et al., 1994) and was

designed to provide a simple, lightweight, general-purpose mechanism for encapsulating data sent over IP internetworks. GRE is a client protocol of IP using IP protocol 47 (Ross, 2001). An acknowledgement bit is used to indicate that a 32-bit acknowledgement field is present and significant (Hanks et al., 1994). The Key field is replaced with a 16-bit Payload Length field and a 16-bit Call ID field. The PPTP client sets the Call ID field during the creation of the PPTP tunnel. A 32-bit Acknowledgement field is added.

2.2.7 Layer Two Tunnelling Protocol (L2TP)

Layer Two Tunnelling Protocol (L2TP) is a combination of Microsoft's PPTP and Layer 2 Forwarding (L2F), a technology proposed by Cisco System's, Inc. L2TP supports any routed protocol such as, IP, IPX, and AppleTalk (Yuan et al., 1998). L2TP can be used as a tunneling protocol over the Internet or private Intranets. PPP defines an encapsulation mechanism for transporting multiprotocol packets across layer 2 (L2), point-to-point links. Typically, a user obtains a L2 connection to a Network Access Server (NAS) using one of a number of techniques and then runs PPP over that connection (Cheung & Misic, 2002). L2TP extends the PPP model by allowing the L2 and PPP endpoints to reside on different devices Interconnected by a packet-switched network. With L2TP, a user has an L2 connection to an access-concentrator and the access-concentrator then tunnels individual PPP frames to the NAS. This allows the actual processing of PPP packets to be divorced from the termination of the L2 circuit (De Clercq & Paridaens, 2002). L2TP uses UDP messages over IP internetworks for both tunnel maintenance and tunneled data. L2TP therefore uses message sequencing to ensure the delivery of messages (Kindred & Sterne, 2001). L2TP supports multiple calls for each tunnel. To identify the tunnel and a call, there is a Tunnel ID and Call ID in the L2TP control message and the L2TP header for tunneled data (Patton et al., 2000a).

2.2.7.1 Tunnel Maintenance with L2TP Control Messages

Unlike PPTP, L2TP tunnel maintenance is not performed over a separate TCP connection (Qu & Srinivas, 2002). L2TP call control and management traffic is sent as UDP messages between the L2TP client and the L2TP server. L2TP control messages sent as UDP datagrams are sent as the encrypted payload of IPSec ESP as illustrated in Figure 2.8 (Yuan et al., 1998). Because a TCP connection is not used, L2TP uses message sequencing to ensure delivery of L2TP messages. Within the L2TP control message, the Next-Received field (similar to the TCP Acknowledgment field) and the Next-Sent field (similar to the TCP Sequence Number field) are used to maintain the sequence of control messages (Box &

Sterling, 2001). Out-of-sequence packets are dropped. The Next-Sent and Next-Received fields can also be used for sequenced delivery and flow control for tunnelled data.

L2TP supports multiple calls for each tunnel. In the L2TP control message and the L2TP header for tunnelled data is a Tunnel ID that identifies the tunnel and a Call ID that identifies a call within the tunnel (Cheung & Misic, 2002)

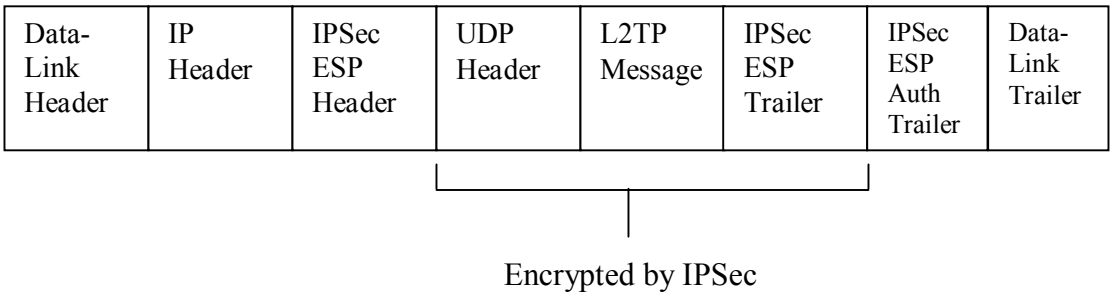

Figure 2.8 L2TP Control Message adopted from Yuan et al (1998, p. 145)

2.2.7.2 L2TP Encapsulation

The initial PPP payload is encapsulated with a PPP header and an L2TP header. The L2TP encapsulated packet is then encapsulated with a UDP header with the source and destination ports set to RFC 1701 (Hanks et al., 1994). Based on IPSec policy, the UDP message is encrypted and encapsulated with an IPSec Encapsulating Security Payload (ESP) header and trailer and an IPSec Authentication (Auth) trailer. The IPSec packet is encapsulated with a final IP header containing the source and destination IP addresses of the VPN client and VPN server.

2.3 CONCLUSION

This Chapter 2 has reviewed the fundamental IT context in which all secure business processes occur. The basic building blocks are the two concepts of network and routing. Special attention was paid to the Virtual Private Network (VPN) as a preferred business IT support for protecting information. The critical review of network literature showed that security was not the focus of both the OSI and TCP/IP networking models. Security was a secondary concern and communication the primary. The research then identified different weaknesses in both models and defined the different attack types that could be expected at different layers and in different models. The generic threats to routing protocols included as followings threat sources, threat actions, and threat consequences. Security issues in IP multicast tended to revolve around the application in use. If part of the network traversed the

Internet, firewalls had to be reconfigured to allow IP multicast traffic through. The IP version upgrade (IPv6) is indicative of more recent concern for security and the protection of information while being broadcast over networks. A supporting example of this was the IPv6 Authentication and Security Encapsulation options.

The problem of information protection has been identified at its lowest IT levels. In Chapter 3 the matters of IT interfacing with business process and the organisational structures is to be addressed. The extended problem of IT objectives, business objectives, and operational, tactical and strategic requirements of organisations are also to be addressed. The role of security standards, control frameworks and the alignment problem are to be located in the literature and discussed. This Chapter has identified the strengths and weakness of IT and the inherit risk IT contributes to and business information environment.

CHAPTER 3

THE BUSINESS IT CONTEXT

3.0 INTRODUCTION

An organization may regard IT as a necessary performance, something that is needed in order to stay in business, while other may see it as major source of strategic opportunity, seeking proactively to identify how IT-based information systems can help them gain a competitive edge. As IT is becoming more powerful, its use has spread throughout organizations at a rapid rate. Different levels in the management hierarchy are now using IT where once its sole domain was at the operational level. The aim now is not only to improve efficiency but it is also to improve business effectiveness and to mange organization more strategically. As the managerial tasks become more complex, so the nature of the required information systems (IS) changes – from structured to unstructured, complex enquiries at the highest levels of management. IT, however, has the potential to change the way an organization works and also the very nature of its business (see, for example, Gibson, 2003). IT can record, synthesize, analyse, and disseminate information quicker than at any other time in history. Data can be secured and collected from different parts of the company and its external environment and brought together to provide relevant, timely, concise and precise information at all levels of the organization to help it become more efficient, effective and competitive. Chapter 2 defined the important issues in the IT context. This chapter is concerned with the business use of technology and charts the evolution of the technology and the types of security technology used by organizations.

Developments in IT have caused revolutionary changes not only for individual organizations but for society in general. With the developments of IT, as with most things, comes the possibility of abuse. Data integrity and security is of prime important to ensure validity and privacy of the information being held. Managing the information involves identifying what should be kept, how it should be organized, where is should be held and who should have access to it. The quality of this management will dictate the quality of decisions being taken and ultimately the origination's survival. This is the subject matter of chapter 3; it describes how the role of IT has changed in business and how organizations have reacted to this change. Major transition points in organizations' usage of IT are identified retrospectively in order to provide a chronicle of events, placing today's developments in a historical context. Such histories are not merely an academic exercise; they can serve as a

foundation for future progress, allowing organizations to avoid past mistakes and to build on their successes.

Chapter 3 is divided into 8 sections. Section 2 puts into perspective the various developments (how the technology itself changed, how organizations have gone about developing information systems, how the role of systems has changed), and to identify trends and key turning points in the brief history of computing. Section 3 focuses on the relationship between IT performance and its evaluation as it is expressed in the debate around what has been called the IT productivity paradox. Section 4 clarifies the linkage between IT and Business and the tested measure of the social dimension of linkage. Information Systems Strategy, section 5, focuses on adjusting IT to business goals and process including case study; it is to provide a frame work into actual practice of information strategy in contemporary organizations. Section 6 briefly reviews interpretation within the IT governance literature. This section examines a control framework of IT governance and the effectiveness IT governance, which can help an organization ensure alignment between use of IT and its business goals. Section 7 identifies business security frameworks and the major drivers for information protection. To construct an effective security policy, technology, business processes, and risks are also taken into consideration.

3.1 THE ESTABLISHMENT OF LINKAGE BETWEEN IT AND BUSINESS

The establishment of linkage between Information Technology and Business objectives has consistently been reported as on the key concerns of information systems (IS) managers. In recent surveys of information systems and business mangers (Galliers, et al., 1994; Niederman, et al., 1991), information technology (IT) planning has consistently been rated as one of their most important concerns. A review of the empirical literature reveals, that on issue, the linkage of IS plans with organizational objectives, has been among the top problem reported by information systems (IS) managers and business executive.

In broader sense, Foss (1997) points that information technology management can conceptualize as a problem of coordinating the relationship between the business domain and the IT domain. In this context, IS planning is only one of several mechanisms that can be utilized to accomplish this task (Foss, 1997). Ackoff (1999) argues that although the need for linkage has been well recognized and companies report low success rates in attaining it, there are few studies of how companies perceive the linkage issue of how they actually organize and act to achieve it. The linkage construct has two dimensions: Intellectual and

Social. It is possible to have clear understanding of linkage and how it is achieved in order to aid organizations whose ability to harness the power of IT is critical to their success.

3.1.1 The Linkage Construct

In order to develop a comprehensive view of linkage, this section (1) defined a broad band of connections between IT and business, from short-term plans to long-term version, (2) differentiated between the cause and outcome views of linkage, and (3) distinguished between the intellectual and social dimensioned linkage. The result of each of these activities is described below.

In the IT literature, the concept of linkage emanates from an IT planning perspective several authors have suggested that IT plans should be linked to other artefacts in business, such as business plans (Calhoun & Lederer, 1990; Lederer & Mendelow, 1986), business strategies (Pyburn, 1983) or business objectives (Galliers, 1987; Zviran, 1990). Because the IT literature is not consistent in describing what IT plans should be linked to, this study includes the broadest possible set of linkages between the function and the business. In the IT literature, there has been little distinction between linkage as an organizational process or as an outcome of these processes. Palshaugen, et al. (1998) view, certain organizational processes lead to the state of being linked. Therefore consider the organizational processes as potential causes of linkage and linkage as the effect (Lee, et al., 1999).

The first attempt to dimensionally link is found in the accounting literature. Shank, et al. (1973) suggested that business plans and budgets could be tightly or loosely linked, depending on three characteristics: (1) content linkage between the plans and budgets, (2) timing linkage between the planning and budgeting systems, and (3) organizational linkage between the people doing planning and budgeting. These three dimensions were adapted by IT researchers (Lederer & Mendelow, 1989), who stated that 'coordination can be achieved in three dimensions-content, timing and personnel'. Using the cause/effect distinction, the content dimension is the effect, and the time and organizational dimensions are potential causes of linkage.

3.1.2 The Intellectual Dimension of Linkage

Horovitz (1984) made an important distinction between the intellectual and social dimensions of the process of strategic business planning. In the Horovitz model, the intellectual dimension refers to particular methodologies, technique, and data used in the formulation of strategy. The social dimension refers to factors such as the choice of actors, their degree of

involvement, and the method of communication and decision making. By applying this distinction to linkage and focusing on linkage as a resultant state, two separate dimensions of linkage are identified. The intellectual dimension of linkage is the state in which IT and business objectives are consistent and valid. The social dimension is the state in which business and IS executives in an organizational unit understand and are committed to each other's mission, objectives, and plans.

Potentially promising strategies and plans may be poorly executed or even subverted because organizational actors are not aware of or are not committed to them. On the other hand, perfect implementation of flawed plan may create suboptimal results. It seems that both dimensions, intellectual and social, are necessary for an organization to make full use of IT in support of, or as a catalyst for, business strategy. By placing the dimensions of linkage on one axis and the cause and effect distinction on another, the result is a frame work (Table 3.1) to guide the study linkage. Factors and process in Quadrant 1 of Table 3 (the influences on the intellectual dimension of linkage) have been studied extensively since the inception of strategic business planning in the mid seventies (Henderson & Venkatraman, 1992).

Until recently, less attention had been paid to describing and measuring the result of these activities (the intellectual dimension of linkage, i.e. Quadrant II). Henderson & Sifonis (1988) provided a framework for this dimension by suggesting that strategic plans need internal consistency and external validity. In the context of linkage, this idea would result in two aspects of the intellectual dimension of linkage:

- Business and IT planning outputs are internally consistent, i.e. the IT mission, objective, and plans chosen are consistent with the stated business mission and objectives.

- Business and IT planning outputs are externally valid, i.e. they are comprehensive and balance with respect to external business and IT environment. For example, if new technology exists that could impact the business strategy; it has been included in the IT strategy.

Table 3.1: Framework for studying linkage of intellectual and social dimensions

	Potential factors influencing linkages	
Dimension of linkage	**Causes**	**Effect**

Intellectual dimension	**I** The methodologies for formulation of IT and business mission, objectives and plans, and the comprehensiveness of the planning activities (J. Henderson & Venkatraman, 1992)	**II** The degree to which the set of IT and business mission, objectives, and plans are internally consistent and externally valid (J. Henderson & Sifonis, 1988)
Social dimension	**III** Choice of actors, timing, decision making, and communication used in the formulation of mission, objectives, and plans for IT and the business (Calhoun & Lederer, 1990; Lederer & Mendelow, 1989)	**IV** The levels of understanding to the business and IT mission, objectives, and plans by IS and business executives (Doll & Torkzadeh, 1987)

Several studies have focused on Quadrant III factors and processes such as top management support (Lederer & Mendelow, 1989), communication of business plans (Calhoun & Lederer, 1990), and planning styles (Pyburn, 1983). One problem with this research has been that the dependent variable (Quadrant IV), whether it was linkage or IS planning success, has been less carefully defined and measured IS steering committees in alignment (Doll & Torkzadeh, 1987). Providing a better understanding of this dimension of linkage is the objectives of this study.

3.1.3 Strategy Alignment

Academics have also devoted attention to the issue of alignment for a long time (Henderson, 1991). Several researchers have investigated the means of attaining alignment and its impact on organizational outcomes (Broadbent & Weill, 1997; Kearns & Lederer, 2003; Luftman, et al., 1993; Sledgianowski & Luftman, 2005). Henderson and Venkatraman (1991) have described for the first time a strategic alignment model (SAM). They have developed it in

response to a rapidly changing environment of businesses. This model is based on the relationship between strategic fit and functional integration. Strategic fit is the ability to make decisions concerning a company's market positioning based on external and internal environment conditions. It enables the company to structure itself in order to execute the positioning strategy. Therefore, it is interplay between business strategy and organisational infrastructure and processes. Functional integration enables organisations to align their functional strategies, structure and processes using not only internal conditions but also recognises the external environment's variables.

Luftman et al. (1999) argue that the strategic alignment framework may not be sufficient to work on any one of these areas in isolation or to only link business strategy and information technology. They point out that the objective is to build an organizational structure and set of business processes that reflect the interdependence of enterprise strategy and information technology capabilities. Broadbent & Weill (1997) took that alignment model and build on it a theory that recommends how technology infrastructure investments should be made in companies to support business strategies. Fundamentally it is a well-defined idea based on the authors' practical experience. Their idea still requires a well thought through strategic planning process that allows for IT to be part of it. Interestingly, the technology infrastructure investments are the most difficult investments to justify in today's companies. The business landscape is changing very quickly. On the other hand technology infrastructure investments are substantial and have to be utilised for extensive periods of time to provide payback.

The alignment of information technology plans with organizational objectives has consistently been among the top concerns reported in surveys of information systems managers and business executives (Fichman, 2001). According to John & Sali (2003), successful firms have invested in IT like everyone else, but have differentiated themselves by viewing the management of information produced by these systems as being of paramount importance. As these organizations identify the relationship between corporate and IT strategies, they use information to integrate and manage this link. Such organizations succeed because of their ability to differentiate themselves from their competitors in this way. This viewpoint is supported by Earl et al. (1995) who maintain that justification for an IT application links to one of the two conditions: either it improves the performance of the current organization or it improves the outlook for new business opportunities and strategies of the enterprise. Lawrence et al (1998) also supports this viewpoint by maintaining that total business integration is a must for businesses that want to succeed in the information age.

Total business integration, in his definition, is the full assimilation and integration of all information assets into the total organization using business need as the primary driver for the processes. Baker (1999) agrees that a total management approach is needed which fully assimilates and integrates all information functions and technologies in the organization.

In the broadest sense, information technology (IT) management can be conceptualized as a problem of aligning the relationship between the business and IT infrastructure domain in order to take advantage of IT opportunities and capabilities (Sabherwal & Chan, 2001). In the research literature, there seem to be two approaches to the subject of alignment. The first concentrates on examining the strategies, structure, and planning methodologies in organizations (Bruce, 1998; Papp, 1999). The second investigates the actors in organizations, examining their values, communications with each other, and ultimately their understanding of each others' domains (Lawton, 2002; Lester & Parnell, 2002).

There is support in the literature for studying the social dimension of alignment. For example, as Cascella (2002) notes, the culture gap between IT and business people has been identified as a major cause of system development failures. Mintzberg (2003) notes that formal planning is not the only way to create strategy. He suggests that relying on the strategic vision and strategic learning approaches, the latter based on integrating the views and visions of a number of actors, is a better means to cope with uncertain environments. Fuchs et al (2000) state that the current planning literature is based mainly on a rational model of organizational decision making. They note, however, that other models such as the political behavioural model or the resource dependency model also provide robust descriptions of the IT planning processes.

Another theoretical perspective supporting the concept of the social dimension of alignment is the social construction of reality (Gyampoh-Vidogah, et al., 2003). This view would suggest that, in addition to studying artefacts (such as plans and structures) to predict the presence or absence of alignment, one should investigate the contents of the players' minds: their beliefs, attitudes, and understanding of these artefacts. This research attempts to measure the executives' understanding of IT and business plans. Other studies have also investigated the social dimension of alignment (McAdam & Bailie, 2002; Sabherwal, et al., 2001). The approach in those studies was to use statistical methods on a large sample in order to measure relationships between independent variables and alignment. A more interpretive approach (Cascella, 2002) is taken here to discover how certain critical factors interact to create conditions that enable or inhibit alignment.

Shared domain knowledge is defined as the ability of IT and business executives, at a deep level, to understand and be able to participate in the others' key processes and to respect each other's unique contribution and challenges. Sabherwal & Becerra-Fernandez (2003) shared knowledge construct, developed concurrently, is very similar, although their operationalization differed. There is evidence in the organizational behaviour literature about the importance of shared knowledge. Nambisan et al.(1999) note that common knowledge improves communication. Chan (2000) posited a relationship between shared understanding and innovation. The shared domain knowledge construct has also been of interest to IT academics for more than a decade. Flynn & Flynn (1999) suggested ways to develop IT-knowledgeable line managers. There is empirical evidence on the importance of shared knowledge for IT-line partnerships (Henderson & Venkatraman, 1999), for IT performance (Venkatraman & Henderson, 1998) and for IT use (Luftman & Brier, 1999). Baker (1999) indicates that increased business knowledge influences IT/business executive relationships.

3.1.4 Management by Objectives

Management by objectives (MBO) was first outlined by Peter Drucker (1954) in his book "The Practice of Management". This management foundation has been developed, challenged, implemented and debated over the years. Objectives and objective setting are targeted towards organisational performance measures rather than motivational goal setting or other approaches to organisational control. As a consequence asserting objective driven control is a contentious position. A review of the arguments against objective organisational control shows that all objectives cannot be measured (hence appraisal systems), that objectives are inappropriate measures in some contexts (hence interpretive schema), that objectives cannot change fast enough to keep up with the business (hence strategic planning quality process systems), and so on (Pearce & Robinson, 1997). What is clear from the management and the management IS literature is that objectives suit particular business contexts, business knowledge groups and business approaches. For example, the setting of financial objectives is an appropriate and attainable activity in the finance division of an enterprise. However, there are contexts, knowledge groups, and business approaches in which the setting and measuring of objectives is difficult and can affect business competitive advantage. For example, the setting and measuring of objectives for human performance in an enterprise maybe precise in a planning document but ambiguous in implementation. Hence, the central focus of my proposed research is contentious and assumptions are to be asserted. For example, the research is asserting that businesses set objectives, that businesses

measure performance, that the alignment of objectives influences competitive advantage, that the attainment of objectives is a capability measure, and so on (the research hypotheses).

Object oriented business planning has received a fresh resurgence with the growth of IT adoption in enterprises. IT has exported a context, a knowledge group and approaches that are often foreign to non-MBO (and other) business cultures. The appeal of IT and its perceived business benefits has out weighted the perceived costs of implementation and enterprises are prepared to go through the risk of cultural change. This is the context in which the research is to take place. The assertion that the worlds of IT and of Business are different is often contested with arguments that one is subsumed by the other or they inter-relate in a symbiotic way (Pearce & Robinson, 1997). The exploration of this relationship is central to the research and its definition critical to the outcomes. The knowledge framework selected for the research (see Appendix B) also divides the research domain into three layers that contain knowledge of different types. The context hence has elements of conceptual abstractions (ie. Philosophy & theories), of structure (ie. Models & design), and of empirical realities (ie. Managerial practice & work systems).

The tenuous relationship between the IT organization and the business presents a major challenge for business organizations, especially in the area of effective security knowledge management. When each side has poor knowledge of each other's issues and there is ineffective communication and critical knowledge sharing cannot occur (Duffy, 2002). This often results in an ineffective alignment of IT solutions and services to business needs (Inayatullah & Leggett, 2002). Inayatullah & Leggett emphasize that symptoms of this misalignment include poor co-ordination of work practices, delays and de-scoping of projects, poor user requirements satisfaction and inflexible information systems. Over time, these issues negatively influence the perceptions that users have of the IT organization as a whole. Organization culture has often been used as a way to explain the gap between business and IT organization, and Gibson (2003) argues that there is clearly a culture gap. Gibson states that it is imperative to seek a better understanding of why the gap exists, its dimensions, and how it can be reduced. The poor alignment between business and IT may be due to the poor knowledge that business staff have of IS functions (2003; Peak & Guynes, 2003). Peak & Guynes have focused on power, claming that the low status of the IT organization is responsible for poor alignment.

3.2 IT GOVERNANCE

The importance of IT governance is a reflection of the change role and relevance of IT within an enterprise and the need to ensure that it is properly managed. While Duffy (2002; 2002) emphasizes, through those changes, "IT becomes not only a success factor for survival and prosperity, but also an opportunity to differentiate and to achieve competitive advantage". This section briefly reviews varying interpretation within the literature. Although aspects of IT governance derive from the controls of internal audit, it should be examined and understood in a wider context. The term is not owned by internal audit although IT governance has an element of internal control and risk management.

At the heart of the governance responsibilities of setting strategy, managing risks, delivering value and measuring performance, are the stakeholder values, which drive the enterprise and IT strategy. Sustaining the current business and growing into new business models are certainly stakeholder expectations and can be achieved only with adequate governance of the enterprise's IT infrastructure (Devaraj & Kohli, 2002). IT governance, like other governance subjects, is the responsibility of executives and shareholders (represented by the board of directors). It is not an isolated discipline or activity, but rather is integral to enterprise governance. It consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives.

The highest profile in developing and communicating this viewpoint of IT governance is the ISACA (Information Systems Audit and Control Association) and the IT Governance Institute it establish in 1998. ISACA defines IT governance as a "structure of relationship and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes". It is not possible to discuss and explain IT governance with just one definition. The literature presents a range of perspectives that represent different understanding. IT governance is the responsibility of the board of directors and executive management (IT Governance Institute, 2001). Van Grembergen (2002) examined IT governance definitions and found that IT governance is the organizational capacity exercised by the board, executive management and IT management to control the formulation and implementation of IT strategy and it this way ensure the fusion of business and IT. Bodnar (2003) feels that when the term "governance" is borrowed and prefaced with IT, some commentators in the IT industry confuse other and possibly even themselves. Ivan (2000) agrees that, at times, IT

governance refers to the IT management architecture or structure. Schwarz and Payne (2003) suggest that, historically, IT governance has been strongly associated with the structure or configuration of the IT function. This is a reflection on locus of responsibility for making IT management decision and is typically described as centralized, decentralized or divided between them as shared federal or hybrid (Ivan, 2001).

However, when Duffy (2002) gives his own definition of IT governance, structure remains an important component although suggesting it has moved beyond structure to embrace relationships. Patel (2002) agrees that structure is an historical perspective of IT governance. While proposing an emergent IT governance structure is required for ebusiness, he refers to the historical phases of IT governance in terms of structure and focus of responsibility. Section 6.1 examines the COBIT as control framework of IT governance, which helps an organization ensure alignment between use of Information Technology (IT) and its business goals.

3.2.1 COBIT Framework

COBIT (Control Objectives for Information and Related Technology) was developed by Information Systems Audit and Control Association (ISACA) and IT Governance Institute a generally applicable and accepted international standard for good practices for IT controls (as compared with ITIL (Information Technology Information Library) that provides controls at some tactical and process level objectives, such as the help desk). COBIT is based on ISACA's existing Control Objectives, enhanced with existing and emerging international technical, professional, regulatory, and industry-specific standards. It was written for three specific audiences' management, users, and auditors.

Hawkins, et al. (2003) stated that COBIT is designed to be an IT governance aid to management in their understanding and managing of the risks and benefits associated with information and related technology. COBIT is independent of the technical IT platforms adopted in an organization; it is an open standard for control over information technology. COBIT is arguably the most appropriate control framework to help an organization ensure alignment between use of Information Technology (IT) and its business goals, as it places emphasis on the business need that is satisfied by each control objective (Tyler, 1999). This section reports on the use of a simple classification of the published literature on COBIT, to highlight some of the features of that literature.

In part as a response to new governance requirements, increasing emphasis has been placed on internal controls in organizations. Controls are activities that are undertaken either

to eliminate risks or reduce them to a level that is considered acceptable (Gaynor, 2002). The rules, policies and procedures involved in managing an organization's risks are considered as the system of internal controls (Lawson, et al., 2003), where internal control is designed to give "reasonable assurance" on the achievement of objectives relating to the "efficiency and effectiveness of operations", the "reliability of financial reporting" and compliance with relevant laws and regulations (Devaraj & Kohli, 2002; Shin, 2003). The development of frameworks of internal control objectives to allow for international standardization has arisen also from pressure by auditors. Without a framework it is difficult for auditors to be able to substantiate their view on internal control (Amaratunga, et al., 2001).

Korac-Kakabadse & Kakabadse (2001) claim that in recent years a range of documents has been issued that aimed to assist with the definition, assessment, reporting on and improvement of internal control in organizations. These include COBIT, Committee of Sponsoring Organizations (COSO), the Institute of Internal Auditors Research Foundation's Systems Electronic Security Assurance and Control (eSAC) and the IT Infrastructure Library (ITIL). Although such documents have been developed to address different needs and audiences, many of them have built on the contribution of previous documents and consider much the same internal control concepts (Inayatullah & Leggett, 2002). For example, amongst others, COBIT has drawn on both COSO and a predecessor of eSAC.

While a range of frameworks, standards and documents related to the control of IT exist; the primary focus of COBIT is on aligning use of IT with the achievement of organizational goals. COBIT is a comprehensive framework of 34 control objectives that has been developed from "41 international source documents" (Guldentops & De Haes, 2002) and validated internationally to help balance IT risk against investment in IT controls. Guldentops, et al. (2002) have identified that the control objectives have been organized into a hierarchy of processes and domains that are designed to help bring about the alignment of business and IT objectives, by identifying the requirements for IT resources and information associated with 318 detailed control objectives. IT processes are grouped into four domains: planning and organization, acquisition and implementation, delivery and support and monitoring (Van Grembergen & Van Bruggen, 2002). As the framework considers all aspects of information and its supporting IT, management can use COBIT to help provide an appropriate control system for IT.

COBIT has been implemented in many countries since its introduction in 1996. Hawkins et al.(2003) claims that organizations where COBIT has been adopted include New South Wales Department of Health in Australia (Tyler, 1999), Royal Philips Electronics in

the Netherlands, Blue Cross Blue Shield of Michigan in the USA (Fedorowicz & Ulric, 1998) and Department of Defense, USA (Zagorsky, 2003). That COBIT seems to be becoming an influential framework for the control and governance of IT is attested to by the significance and diversity of the organizations in which it has been utilized. Furthermore, as COBIT is currently in its 4th edition, and a version for Small to Medium Sized Enterprises called "CobiT Quickstart" has been released in 2003, VALIT in 2006, and version 4.1 in 2007. Such developments further indicate COBIT's influence (Guldentops & De Haes, 2002).

In the literature reviewed it appears that relatively little academic literature has been published that investigates the utilization of COBIT. Patel (2002) argues that may be because the extensive electronic sources available on COBIT are primarily designed for IT and audit practitioners. Hawkins et al.(2003) claim that these sources are produced by Information Systems Audit and Control Association (ISACA) and the IT Governance Institute and are not referred to by many academic authors. Damianides (2004) claimed that studies that have benchmarked the adoption and use of COBIT have been published. Apart from the excellent case studies produced by the IT Governance Institute, there is little literature that considers the range and characteristics of organizations that have utilized COBIT and the outcomes of implementation. If it can be established that implementation of COBIT is related to more effective IT governance, as it is hoped, then analyses of cases of both successful and unsuccessful implementations will lead to a better understanding of current best practice (Damianides, 2004).

Moreover, analysis of the extent of implementation by organization and industry, and categorization by size, sector, and geographic area and so on, will be valuable in helping to identify trends. In turn, the results of such analyses will help to identify organizations with the greatest and least need for public and private sector investment in IT governance in the future, and as a consequence, lead to more effective targeting of expenditure. To date it appears that only limited examination of the published literature on COBIT has been reported. Because much of the literature that is available on COBIT appears to have a practitioner focus, and has been made available through a range of often non-academic forms. The literature is not as accessible as that available in other areas that have been investigated intensively by academic researchers. Consequently, there is a need to synthesize and characterize the literature that does exist.

3.2.2 IT and Corporate Governance

The appropriate alignment between use of IT and the business goals of an organization is fundamental to efficient and effective IT governance. IT governance is the structure of relationships and processes to develop, direct and control IS/IT resources in order to achieve the enterprise's goals. IT governance has been recognized as a critical success factor in the achievement of corporate success by deploying information through the application of technology. Lucas (1999) claims that the importance of IT governance can be appreciated in light of the Gartner Group's finding that large organizations spend over 50% of their capital investment on IT . However, research has suggested that the contribution of IT governance varies in its effectiveness (Gaynor, 2002). IT control frameworks are designed to promote effective IT governance.

IT governance usually occurs at different layers, with team leaders reporting to and receiving direction from their managers, with managers reporting up to the executive, and the executive to the board of directors. Reports that indicate deviation from targets usually will already include recommendations for action to be endorsed by the governing layer. Clearly this will not be effective unless strategy and goals have first been cascaded down into the organization.

The governance process starts with setting objectives for the enterprise's IT, providing the initial direction. From then on, continuous loops are established of performance that is measured and compared to objectives, resulting in redirection of activities where necessary and change of objectives where appropriate. While objectives are primarily the responsibility of the board and performance measures that of management, it is evident they should be developed in concert so that the objectives are achievable and the measures represent the objectives correctly.

The ultimate reason IT governance is important is that expectations and reality often do not match. Payne (2003, p. 45) identifies that boards usually expect management to "Deliver quality IT solutions on time and on budget", "Harness and exploit IT to return business value", and "Leverage IT to increase efficiency and productivity while managing IT risks". The reasoning behind the first general hypothesis is that organizations must implement controls to prevent, detect, and correct deviations from approved information technology processes to realize the benefits of implementing these best practice processes. For example, an organization might institute a change management process that requires that a change management committee authorize all changes to critical web servers and that any subsequent

changes be verified against the original request for change. The prediction of this research is that without formal IT controls in place, this process will not achieve its desired outcome, that is, unauthorized changes will occur and cause an increase in server downtime. A preventive control in this example would be to require a change management authorization code before allowing any changes to a server. A detective control would be software that detects any changes to the web server and sends a message to an appropriate person. A corrective control would be the ability to rollback an unauthorized change.

Effective and timely measures aimed at addressing these top management concerns need to be promoted by the governance layer of an enterprise. Hence, boards and executive management need to extend governance to IT and provide the leadership, organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives. IT governance is not an isolated discipline. It must become an integral part of overall enterprise governance, similar to the need for IT to become an integral part of the enterprise rather than something being practiced in remote corners or ivory towers.

An increasingly educated and assertive set of stakeholders has raised concerns about the sound management of their interests. This has led to the emergence of corporate governance regulations and standards for overall enterprise governance. These regulations establish board responsibilities and demand that board directors exercise due diligence in their roles of setting strategy and ensuring management implements it.

Enterprise governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly.

IT is essential to manage transactions, information and knowledge necessary to initiate and sustain economic and social activities. These activities increasingly rely on globally cooperating entities to be successful. In many organizations, IT has become an integral part of the business and is fundamental to support, sustain and grow the business.

Many organizations recognize the potential benefits that technology can yield. Successful organizations understand and manage the risks associated with implementing new technologies. Too often, however, there is lack of understanding of how strategically important IT is to the organization.

3.3 BUSINESS SECURITY FRAMEWORK

For many organizations, information security is becoming the most critical information technology-related challenge they face. Information security has many different facets, but the main goal is protecting the confidentiality, integrity, and availability of an organization's information assets. Security is defined as a combination of systems, operations and internal controls to ensure the integrity and confidentiality of data and operation procedures in an organization (Baltatu, et al., 2000). A violation of any of these components can quickly put an organization at risk, both legally and to its reputation. For any organization, the information system is valuable and should be appropriately protected. Cusack and Sirisukha (2003) state that the IS includes information, the physical assets, the human resources and the symbols that represent capital value.

The importance of information security in a computer-based environment has resulted in a large stream of research that focuses on the technical defences, for example encryption, and access control (Hicks, et al., 2003), associated with protecting information (Al-Khayatt, et al., 2002; Brendon, 2002; Rosenbaum, et al., 2003). In addition, Baskerville and Portouga (2003) claim research has been rapidly developing that focuses on the behavioural aspects of reducing information security breaches.

Dhillon and Backhouse (2000) studied developing, implementing, operating, and reviewing an information security department, the mission of that department must be to support the business objectives of the larger organization. Brooks, et al. (2002) stated that the degree to which this occurs affects the perception, acceptance, and effectiveness of the information security department. Therefore, Kolokotronis, et al. (2002) argued that the information security department's place in the organization must be at a sufficiently high level to maximize its effectiveness. For example, in the majority of organizations, the manager or director of information security reports to the chief information officer (Kolokotronis, et al., 2002). This places the director of information security at the same reporting level as the director of computer operations, or other corporate directors. This helps to ensure the visibility and influence of the information security department.

Abu-Musa (2002) claim that the success and effectiveness of an information security department is largely dependent on the support of the senior management and the department's location in the organizational hierarchy. Other contributing elements of success are the staffing of the information security department and its internal structure. Furthermore, Siponen (2002) points out that the information security organization must be equipped to

support and respond to many different needs. This includes not only the technical security area, but also project management, security awareness and training, policy development, application development, and other business-oriented functions (Quinn & Brill, 2002). The skill set of the security organization therefore must be varied. This implies that training and skill development must be addressed differently for the various roles within the organization.
The information security framework deals not only with computer security but it addresses information security (Hazari, 2002). Chi et al.(2003) asserts this implies several areas outside the technical realm and places the framework in the risk management arena. Risk management includes many areas, one of which is security (Cusack & Sirisukha, 2003). Curtis et al.(2003) claim that the purpose of creating a diverse security team is to address security from all directions including the mix of people, policy, and technology. The staffing of the security team, therefore, Ramanujan et al (2002) argue should be commensurate with the needs of the organization. Warren and Hutchinson (2003) state that, this may lead to the increased cooperation or leveraging of other skills within the organization, including the internal audit or the traditional physical security departments. The objective, though, of creating a diverse collection of security professionals within the team is to expand the scope of security into other areas of the organization (Lewis & Byrd, 2003). This will lead to an integrated enterprise-level approach to security and get to the non-technical issues that have sometimes been ignored in the development of security organizations.

The inside of the information security framework can be divided into three major sections: the decision drivers, a development phase, and an implementation phase (Abu-Musa, 2002a; Kesh, et al., 2002; Slay, 2003; Warren & Hutchinson, 2003). These three sections allow the framework to be broken into manageable, logical divisions.
Decision Drivers: this section of the internal framework brings together the major drivers for information protections, which are used as "inputs" to the development section of the framework. To construct an effective security policy, technology, business processes, and risks must be taken into consideration. By analysing technology strategy and usage, business initiatives and processes, and vulnerabilities and risks, the framework documents the need for information security within an organization. This "measurement" of the major forces behind information protection provides valuable insight as the architecture is assembled. It also identifies major areas within the organization that should be addressed from an information protection angle.

Development: to be effective, corporate security strategy must be applied to applications and technical platforms. There must be a stage of planning and development as

this strategy is created. The combination of "decision drivers" and comprehensive security practices form the first component of the development phase the security policy.

Implementation: implement operating system and application technical control standards to support the corporate security strategy. This ensures that the organization's security architecture will be as efficient and effective as possible while taking an enterprise-level view.

3.4 IT SECURITY STANDARDS

This section discusses the following security standards and documents: ISO 17799, ISO 15408, SP800-14, SP800-27 and SAS94. These are widely used and respected standards and documents published by recognized organizations and government agencies. Both It and business recognise the benefit of using standards for IT management and IT security. It is a necessity for an organisation when it decides to outsource part of its business. Using a publicly available standard as the basis for service level agreements between the organisation and its business partners may lead to less misunderstanding and lower associated costs (McAdams, 2004). A standard recommends establishing and maintaining a documented information security management system. This system should focus on identifying critical information assets, specifying the degree of assurance required as well as risk management, control objectives and procedures (Wool, 2002).

3.4.1 ISO 17799 Information Security

The international organization for standardization issued the code of practice for information security management (ISO 17799) in 2000. This standard is based on the British Standard 7799 first published in 1995 (Kenning, 2001). It is a comprehensive set of controls considered to be best practices in information security including policies, practices, procedures, organizational structures and software functions. The section on system development and maintenance provides specific security objectives, risks and controls relevant to application security. Business process analysis is suggested in the initial phases of implementation to identify, justify and document the requirements of the application. The basic objective of application security according to ISO 17799 is to prevent loss, modification or misuse of user data. Controls should be designed around the input, processing and output of data (Mercuri, 2003).

Specific input controls include dual input checks, where data are entered repetitively and then compared for errors. Detection of such errors as out-of-range values, invalid

characters in data fields, and missing or incomplete data is an objective. The processing of data should include controls to protect the integrity of the data. Examples of such controls are batch totals before and after processing, balance controls to check opening balances to previous closing balances, checks on the order of processing programs and whether programs are terminated or halted in the case of a failure. Output controls may include plausibility checks to test whether output data are reasonable and reconciliation control counts to ensure complete processing of all data.

Cryptographic controls are discussed with the objective of protecting the confidentiality, authenticity and integrity of information. Policies are appropriate here to identify sensitive information that requires strong protection. Encryption algorithms and length of cryptographic keys are important issues. Digital signatures and cryptographic key management are controls to protect the authenticity and integrity of electronic documents. Key management includes the critical functions of generating, distributing, storing and revoking keys.

3.4.2 ISO 15408 Information Security

ISO 15408 is based on the common criteria for evaluating IT products and systems. The common criteria function is a standard for measuring the security and assurance associated with a product. The objective is to prevent unauthorized disclosure, modification or loss of use--similar to confidentiality, integrity and availability. The original Common Criteria for Information Technology Security Evaluation was published in 1999 by a consortium of US and European national standards organizations and licensed to the ISO as ISO/IEC 15408 (Iyengar, 2004).

Evaluations of IT products using ISO 15408 can be used as assurance about the security of a product or as a guarantee by the manufacturer about security capabilities. Consumers can use the standard to determine if an application or system fits their requirements. Developers use the standard as a guide in designing and building a product. Evaluators use the standard to test products and to determine what functionality is included.

Organisations wishing to adopt IT best practices need an effective management framework that provides an overall consistent approach and is likely to ensure successful outcomes when using IT to support the enterprise's strategy.

Assurance requirements are based on confidence in the implementation of security functions as well as the effectiveness of the security functions. These requirements are based on the presence of the desired behaviour as well as the absence of undesired behaviour. The

eight assurance requirements are configuration management, guidance documents, vulnerability assessment, delivery and operation, life cycle support, assurance maintenance, development and testing.

3.4.3 SP 800-14 Application Security

The National Institute of Standards and Technology (NIST) in the US Department of Commerce published the Generally Accepted Principles and Practices for Securing Information Technology Systems, Special Publication (SP) 800-14, in 1996. The document provides a baseline for developing and reviewing IT security programs. The eight principles and 14 practices in the document are applied in the use, protection and design of government information and data systems (Brooks, et al., 2002).

Application security is addressed in specific practices such as life cycle planning and security considerations in computer support and operations. The practice of life cycle planning for computer application software includes the five phases: initiation, development/acquisition, implementation, operation and disposal. Each phase is described with security requirements, which can be technical features, assurances or operational practices. During the initiation phase, a sensitivity assessment should be performed. In the development/acquisition phase, security requirements should be documented and incorporated into specifications. In the implementation phase, testing should be conducted and accreditation sought from management. In the operations phase, security operations should be continuous with appropriate monitoring and auditing. In the disposal phase, data should be removed and the media sanitized.

3.4.4 SP 800-27 Application Security

SP800-27 includes 33 security principles that apply to the life cycle planning phases discussed in SP800-14. Almost all of these principles are relevant to application security. The first principle is to establish a security policy as a foundation for design (Haworth & Pietron, 2006). The following principles deal with policy, risk and characteristics of good security, simplicity. Additional principles discuss access controls, data management and the training of developers in security techniques.

3.4.5 SAS 94 Application Security

The AICPA Auditing Standards Board issued The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit (SAS 94) in 2001.

This standard requires financial auditors to consider information technology as part of overall internal control. Auditors must understand applications and systems in assessing risk and evaluating the integrity of financial information (McAdams, 2004). This standard has therefore brought fundamental concepts of information security and, specifically, application security to the auditing profession.

SAS 94 updates two previous standards, SAS Nos. 55 and 78, on the Consideration of the Internal Control Structure in a Financial Statement Audit. SAS 94 recognizes the larger role of technology in financial reporting. Internal control in this context refers to automated and manual procedures used in preparing financial statements and related disclosures. The specific procedures relevant to auditors include transaction entries into the general ledger as well as journal entries required on a recurring and non-recurring basis. The entire sequence of initiating, recording and processing journal entries should be understood as part of a financial audit.

3.5 CONCLUSION

This chapter has considered the relationships of information technology to organization structure, and the issues associated with information technology performance in an enterprise system. The IT productivity paradox; and organizational design have also been discussed. The more important aspects of each topic have been addressed, while at the same time providing references to other important research work. The various developments (how the technology itself changed, how organizations have gone about developing information systems, how businesses have organized information systems support services, how the role of information systems has changed) have been defined, and trends and key turning points in the brief history of computing located. Separated technologies converged into information technology, and an explanation has been given to clarify the linkages between IT and business. The strategic nature of the business IT relationship has also been elaborated.

The implication of the literature reviewed is that IT functions in a context. The scope and relations within the context were complex, and the explanations were as much theoretical as practical. For example the strategic alignment model reviewed demonstrated how to mange complexity and how to conceptualise solutions. The IT productivity paradox provided another critical edge where the performance in context issue could be discussed. Ways related to improved planning, managing and using IT were elaborated. An element of the IT productivity paradox has been configured out of difficulties and limitations in measuring and

accounting for IT performance. Likewise, the concept of linkage discussed how to improve the planning process so that an apparent link was achieved. Research on the nature of the link, on evaluating whether indeed such a link was present, and from whose perspective, were relatively scarce. This is probably due to the difficulty of operationalizing the link. Finally, the academic community often bemoans the fact that organizational level impact studies of IT are eschewed by virtue of the difficulty of isolation. The problems such as the lag of IT implementation and impact, the isolation of only the IT impact exclusive of any other concurrent organizational change, and the definition of the IT itself, present challenges for researchers. Few empirical studies of the organizational impact of IT were found, especially those that might be suitable to replicate.

The Chapter concluded by considering the current trend to address the control of IT from the highest levels in an enterprise system. IT governance provides a comprehensive framework in which to conceptulise and to implement business control over IT. The global standards frameworks also provide specific detail on how to protect an enterprise IS. The business purpose is to extract financial value from the IT investment and consequently to set objectives that must achieve the business outcome. IT however has the task of achieving the business objectives and also the IT objectives. The two sets of objectives intersect but neither set is a super-set of the other. As a consequence the problem of alignment remains and partially mitigated by for example, the COBIT control framework. This Chapter has laid an important foundation in the thesis. In Chapter 2 the security problem was viewed exclusively from the IT perspective and defined in technical control terms. The security problem has now been elaborated as an enterprise wide problem and made comprehensive by teasing out the business implications of IT adoption. Chapter 4 can now focus onto how others have researched IS problems in this comprehensive context. The research questions arising from these two chapters and the hypothesis generated can be then summarised. A working methodology can then be defined.

CHAPTER 4

RESEARCH METHODOLOGY

4.0 INTRODUCTION

This study employs both quantitative and qualitative research methodologies within the quantitative paradigm to investigate the business and information technology user's perception of Virtual Private Network (VPN) functionality. The preferred approach is best described as a hybrid model and is in keeping with other researchers approaches in the Information Systems literature. The strength of the approach is the inclusion of a greater range of data type and hence to include a wider range of evidence that may be used to accept or reject hypothesis. A weakness is that precise distinctions may be blurred in the grasp for greater contextual evidence. The one shot one target approach to research has been minimised by appeals to realism and other reality checks since the 1990s in the IS literature. The purpose of this chapter is to discuss the various research approaches, the strengths and weaknesses of each proposal, and then to select a preferred research approach that adequately answers the research question.

Information security technologists and business scholars are motivated by a desire to understand how and to what extent the application of IT within enterprise systems leads to improved and secured organizational performance. Researchers have adopted diverse conceptual, theoretical, and analytic approaches and employed various empirical methodologies at multiple levels of analysis (Brynjolfsson & Hitt, 1998). Moreover, the literature includes contributions from several academic disciplines in addition to information systems, including management, strategy, computing, and operations research. In addition, as quantitative information system research has evolved beyond examining the productivity paradox to explore how enterprises use IT to generate value. The limitations of inward looking studies into factors related to low aggregate productivity growth during a period of high IT spending has become apparent, and the ground breaking move towards external as well as internal perspective analysis of enterprise systems has opened the way for data-driven discussion of organisational effects. The consideration of effectiveness as well as efficiency within the context of a real enterprise system world has placed new demands on researchers. The construct of metrics such as cost reduction and productivity enhancement in the assessment of a given business process neglects key enterprise system performance measures from the external perspective (Hitt & Brynjolfsson, 1996). The internal perspective that employs such metrics inadequately treats the external effectiveness of the enterprise system

in relation to market, and organisational objectives in relation to a system's external environment. Hence the issue of competitive advantage finds little redress in real terms (Willcocks, et al., 1996).

IT may enable an enterprise to improve efficiency regardless of whether it is mimicked by competitors, or may yield various performance impacts unique to a particular enterprise relative to its competitors. Synthesizing these observations, information security technology can be defined as the organizational performance impacts of information technology at both the intermediate process level and the organization wide level, and comprising both efficiency impacts and competitive impacts. In this chapter the issue of enterprise systems performance measures is taken up from the methodological perspective and in the context of contested philosophical theories. The position taken is that there are no enterprise foundations in the IS world that give unconditional preference to any particular research approach and that the researcher may select and justify a research approach on various grounds. Consequently, the first section of the chapter discusses different research approaches in the IS world. The second section selects six relevant but different published studies to identify preferences and choices researchers make. In the light of these reviews and the literature reviews in Chapters 2 and 3 a researchable question is identified to guide inquiry into the enterprise system effects of VPN technology. A full data map is provided in Figure 4.7. The research design and its elements are then defined for field research. To conclude the chapter the limitations of the preferred research approach are discussed and the theoretical outcomes from such an ensemble of preferences forecasted.

4.1 IS RESEARCH METHODOLOGY

The concepts of research approach and research methodology are often separated by aligning the approach with a preferred philosophical perspective, and the methodology with a choice (or sequencing) of preferred methods. In judging the validity of researcher choices, consistency is looked for between the research approach and the methodology. As a consequence a researcher may adopt an approach and then select methods that best suit the philosophical perspective rather than being constrained within a traditional interpretation of research approach of either being quantitative or qualitative. Hence the notion of hybrid methods (Markus, 1999) arises where in a traditional sense quantitative and qualitative methods are mixed to achieve the proposed research outcomes. (This concept of mixed methods is also termed ‘triangulation’, (Mingers, 2001)). For example a qualitative study may use surveys or interviews as method and similarly a quantitative study the same. Both

may use statistical analysis to process the data but the way each uses the data will be different. Generally a quantitative study will use deduction or inference to explain substantiative issues on statistical grounds. The qualitative study will generally take the data and interpret it in relation to other data types and look for explanation within the context of the event. Myers (1997, p. 2) puts it this way:

> "**Quantitative research methods** were originally developed in the natural sciences to study natural phenomena. Examples of quantitative methods now well accepted in the social sciences include survey methods, laboratory experiments, formal methods (e.g. econometrics) and numerical methods such as mathematical modelling. **Qualitative research methods** were developed in the social sciences to enable researchers to study social and cultural phenomena. Examples of qualitative methods are action research, case study research and ethnography. Qualitative data sources include observation and participant observation (fieldwork), interviews and questionnaires, documents and texts, and the researcher's impressions and reactions."

The distinction that Myers (1997) and others make between different research approaches is at the philosophical preference level. Attempts to categorise research approaches in IS have also been published (for example, Mingers, 2001, 2003) that locate difference at the philosophical level in distinct categories termed, "positivist", "interpretivist", and "critical" (Chua, 1986). The distinctions between each category are given in descriptive terms. For example, a positivist position considers:

> "Positivist studies generally attempt to test theory, in an attempt to increase the predictive understanding of phenomena. In line with this Orlikowski and Baroudi (1991, p.5) classified IS research as positivist if there was evidence of formal propositions, quantifiable measures of variables, hypothesis testing, and the drawing of inferences about a phenomenon from the sample to a stated population." (Meyers, 1997, p. 3).

An interpretivist position is different. "Interpretive studies generally attempt to understand phenomena through the meanings that people assign to them and interpretive methods of research in IS are 'aimed at producing an understanding of the context of the information system, and the process whereby the information system influences and is influenced by the context' (Walsham 1993, p. 4-5)." And similarly with critical research philosophical

assumptions, "The main task of critical research is seen as being one of social critique, whereby the restrictive and alienating conditions of the status quo are brought to light. Critical research focuses on the oppositions, conflicts and contradictions in contemporary society, and seeks to be emancipatory" (All quotes, Myers, 1997, p. 4). These descriptions are indicative of attempts by researchers to explain difference in research approaches in IS and to provide meta frames in which differences may be justified. In Figure 4.1 Choudrie & Dwivedi (2005, p. 4) structure two prior attempts to frame IS research approaches.

Research Philosophy	Mingers' (2003) classification of research methods	Galliers' (1992) classification of research methods)
Positivist	Observation (passive), measurements, and (statistical) analysis	Laboratory experiment
	Experiments	Field experiment
	Survey, questionnaire, or instrument	Survey
	Case study	Case study
		Theorem proof
		Forecasting
	Simulation	Simulation
Interpretivist	Interviews	Subjective/argumentative
	Qualitative content analysis	Reviews
	Ethnography	Action research
	Grounded theory	Descriptive/interpretive
	Participant observation	Futures research
		Role/game playing
Methods involving interventions	Action research	
	Critical theory	
	Consultancy	

(Adapted from Galliers, 1992; Mingers, 2003)

Figure 4.1: Categorising IS Research Approaches (Choudrie & Dwivedi, 2005, p. 4)

In information systems research, there has been a general shift in IS research away from technological to managerial and organizational issues, hence there is an increasing interest in the application of qualitative research methods. Although most researchers do either quantitative or qualitative research work, some researchers have suggested combining one or more research methods in the one study as a triangulation or hybrid methodology. Recent research on the publication of MIS studies in seven selected top Journals (1998-2003 sample, published 2004) shows that the use of qualitative methods is increasing but that survey and mathematical modelling are still the predominant methods being used (Palvia et.al., 2004). Figure 4.2 gives a summary of these results.

Methodology	Frequency	Percentage
Survey	273	21.3%
Mathematical Model	160	12.5%
Speculation/Commentary	151	11.8%
Laboratory Exp	118	9.2%
Framework & Conceptual Models	110	8.6%
Case Study	105	8.2%
Field Study	88	6.9%
Interview	68	5.3%
Secondary Data	66	5.2%
Literature Analysis	46	3.6%
Content Analysis	33	2.6%
Field Experiment	32	2.5%
Library Research	20	1.6%
Qualitative Analysis	10	0.8%
Total	1280	

Figure 4.2: Methodology Frequency (Palvia et al., 2004, p. 5)

The question of methodology is hence construed to be one of methods choice in this thesis (in keeping with Choudrie & Dwivedi, (2005, p. 4) rather than Palvia et.al., (2004, p. 5). This view allows for the construct of a methodology from any number of methods and its application as specified by the researcher, rather than the constraints of traditional preferences and adherence to strict quantitative and qualitative divides. The expected outcome is that the preferred methodology can reflect best practice and deliver data that may be quantified but with consideration of the MIS context. The following subsections define umbrella groups for the clustering of methods and then address the question of quantifying different data type.

4.1.1 Empirical Methods

Empirical methods are often confused with positivism but the two are distinct constructs that abridge many versions of each (Popper, 1963). Empirical methods may be positivistic or not, and are better defined by the framework in which they occur. An empirical approach to research assumes that the theory comes first and the data second. Data is collected in many ways and then it is analysed for patterns, relationships and clues about the world in which it was collected. Generally empirical methods are classified as part of scientific methods and are related to experience or real data. Bridgeman & Holten, (2000) put it this way:

> "[Empirical methods are] generally characterized by the collection of a large amount of data before much speculation as to their significance, or without much idea of what to expect, and is to be contrasted with more theoretical methods in which the collection of empirical data is guided largely by preliminary theoretical exploration of what to expect. The empirical method is necessary in entering hitherto completely unexplored fields, and becomes less purely empirical as the acquired mastery of the field increases. Successful use of an exclusively empirical method demands a higher degree of intuitive ability in the practitioner." (Bridgeman & Holten, 2000, p. 7)

Empirical research usually starts with the analysis of literature, and then the choice of research questions and hypothesis. The empirical method is applied to collect data that will test theories and conjecture. The notion of theory is such that it may be an established theory proposed by another researcher or it may be theories made up by the researcher but either way it emanates from the reading of literature. The only variation to this is where grounded theory approaches are used to first to develop theories. The use of empirical methods can be interpreted as either in the quantitative or qualitative ways. Methods using experiment, survey, or historical data would be interpreted as being quantitative, whereas case study or action research would be interpreted as qualitative (Moody, 2003, p. 2).

4.1.2 Descriptive Methods

Descriptive methods are used to gain insight into relationships but not to prove causal relationships. The types of relationships that may be explored using descriptive methods are usually behavioural or with grouped data such as time based series. The behavioural studies are the most relevant to contexts that involve human interaction between humans and also inanimate objects such as computers and software. Descriptive methods hence provide insight into events where a participant may demonstrate or declare the occurrence of a target variable. Data may be collected using naturalistic (non-participant or count) method, survey

method or correlation method. The outcomes have explanatory power for matters of prediction and control of contextual (or grouped) events. The descriptions of events (or target variables) provide story lines and network explanation of relationships that are contextually (or grouped) related, and the explanation provides reason (or grounded speculation) for justifying beliefs. Hence description, prediction, explanation and control are expected outcomes when descriptive methods are used.

The notion of descriptive method is used in two ways. First to include contextual data, and the other to include grouped numerical data. The former is generally a qualitative approach and the latter a quantitative approach to research. In the IS literature both notions are applied. Keen (1981) differentiates the descriptive and prescriptive methods to contrast two different ways of collecting and processing data. He uses Mintzberg's 1973 study of managerial work as an example of a descriptive study that came to different explanatory conclusions than a prescriptive study that used the same data. He argues that, "Almost every descriptive study of a complex decision process suggests that formal analysis of quantified information is, at best, a minor aspect of the situation. … Many descriptive models of decision making imply that 'better' information will have virtually no impact." (pp. 24-25). It is in this sense that descriptive methods add value to the array of different research approaches.

4.1.3 Interpretive Methods

Interpretive methods are found in many different areas of research. For example interpretive methods can be applied in history, nursing, psychology, biology and other sciences. The value of an interpretive method is found in the capability of the researcher to explain phenomena in relation to a preferred theoretical framework. In IS the interpretive method can provide contextual linkage between an observed human behaviour and an IS artefact, such as a work surface or hardware. The interpretive element in research opens space for different theories and beliefs to be exercised to explain phenomena. For example, a scientist may construct different models that best interpret observed and theorised patterns or a social scientist use the readings of a preferred philosopher. The method associated with the interpretive element conforms to the adopted philosophy so that for example, an interpretive method associated with Habermas's philosophy of research would conform to hermeneutic traditions of use and explanation. Similarly an interpretive method such as narrative could be chosen to ambiguously exploit the explanatory power of several philosophers.

Nandhakumar & Jones (1997) go to exhaustive lengths to define and then to divide interpretive methods into distinct groups and effects. The key argument is that IS researchers have preferred to distance themselves from the research phenomenon. Interpretive research is a return to engagement and participation by the researcher in the complete context of IS. The case is that "the relationship between the researcher and the phenomena he or she is studying is central to the interpretive endeavour" (p. 110). The IS world is divided into three interpretations, namely that of 'external realism' (positivist approach), 'internal realism', and 'subjective realism'. Interpretive methods address the latter two ontologies (p. 110). In essence interpretive methods are either anti-positivist or normative in effect and are value engaged. The application of interpretative methods provides explanatory power for phenomenon in networks and in terms of the context in which the phenomenon occurs. Knowledge can be transferred through discourse, stories, and other social media. A full range of data collection (or gathering) techniques may be used but a preference for engaged techniques (such as participant observation) would be expected.

4.1.4 Hybrid Methods

Hybrid methods have been developed to incorporate qualitative and qualitative methods within the same study (Mingers, 2001). The extent that either method or number of method are used does not determine if a study is qualitative or qualitative but rather the choice of philosophical position or approach determines if a study is quantitative, qualitative or hybrid. The ways quantitative and qualitative methods are put together are also a matter for the researcher to decide. Often the term 'triangulation' is used to express the relationship of three different methods in practice (Kaplan & Duchon, 1988). Triangulation can be defined as "using multiple techniques within a given method to collect and interpret data." (Jick, 1979, p. 603), and also alternatively case studies "using multiple methodologies in the study of the same phenomenon." (Jick, 1979, p. 602). Hence a hybrid method can be applied at data level or at methodology level to gain quantitative and qualitative perspectives within the same study. The strengths and weaknesses of the approach are evident. A singular study has the capacity to define and locate specific targets with great accuracy, and a hybrid study has the capacity to compare the specific targets in different ways so as to gain a comprehensive view of the target.

The foundational IS example of a hybrid research approach was published by Markus in 1994 in a study of that examined "how and why managers use electronic mail" (p. 502). The information systems context was interpreted to be in a "multi-theory" perspective, and

the best approach for research was to be "multi-method" (p. 503). The multi-method or hybrid approach was justified by the concern that the three alternative perspectives available for structuring an investigation into the context all had serious short comings when addressing the research question. These short comings included bias. Hence statistical survey, inductive analysis, interview, and interpretative methods were triangulated (p. 510). Data was primarily collected from pencil and paper surveys, archival sources, and by interviews (pp. 510, 513, 514). This foundational IS study provides an accepted example of a hybrid approach to field research in IS studies. It also demonstrates the possibility of multiple methods within the same study and potential gains in explanatory power for IS researchers.

4.1.5 Quantification of Data

A field study inevitably involves collecting data according to the choice of data collection methods. Data is hence a selection of the possible phenomena and a representation of reality according to the preferred research framework. The way data is processed may be classified into quantitative or qualitative (although the preference at this level does not determine if the overall approach is quantitative or qualitative (as discussed above)). Data may however be quantified at this level with the use of different techniques. For example coding frames may be adopted and refined to organise collected data and then meta-analysis could proceed using either statistical or relational tools. Another approach would be to select a reliable data processing tool that had been validated and proved in practice by others. The Likert and AHP tools are examples of this second approach. The two issues arising concern the emphasis on quantitative data and also the emphasis on positivist philosophy. Quantification methods and techniques tend to create quantities in the sense that numbers come to represent values. The levels of theoretical constructs, concepts and the interpretation of the numbers are viewed as strong scientific evidence of how a phenomenon works. Quantification hence tends to rely on statistical tools and packages that are an essential element in the researcher's toolkit. Sources of data are of less concern in identifying an approach as being quantitative than the fact that empirically derived numbers lie at the core of the scientific evidence assembled. A quantitative researcher may use archival data or gather it through survey method. In both cases, the researcher is motivated by the numerical outputs and how to derive meaning from them. This emphasis on numerical analysis is also a key to the second issue, positivism, which defines a scientific theory as one that can be falsified.

Quantitative is orthogonal to the analytical modelling that typically depends on mathematical derivations and assumptions. This difference stresses that empirical data

gathering or data exploration is part and parcel of quantitative, while the positivist philosophy deals with problem-solving and the testing of the theories derived to test these understandings. It is also not design research, in which IT artefacts are designed to improve processes. Models and prototypes are frequently the products of design research. In quantitative, the models employed are most often causal models whereas design research places its stress on ontological models. There is also the difference that quantitative validates its findings through data whereas design research can find acceptable validation of a new design through a mathematical proof of concept. Nevertheless, it should be noted that design researchers are increasingly using quantitative, specifically experimentation, to validate their models and prototypes so quantitative is also becoming a key tool in the ways of design researchers.

Several reviews of the literature focus on studies using quantitative empirical methodologies. Conceptual and theoretical studies apply theory and grounded observation to explicate business and IT. Analytic studies utilize game theory and other modelling techniques to develop models of business and IT whose solutions inform understanding of the organizational performances and the competitive environment. Empirical studies also include qualitative research case studies and field studies and quantitative studies estimating IT and business at the process, business unit, enterprise, industry, and country levels of analysis. Combining these observations, quantification may provide the raw data for any of these research elements.

The incorporation of multiple modes of analysis into the design allows additional insights to be potentially revealed that would otherwise remain undiscovered via a single methodological approach. Using multiple methods increases the robustness of results because findings can be strengthened through cross-validation. This can be achieved when disparate data sources converge or when an explanation is developed to account for the data when they diverge. Comparison is a key technique. Good examples of combining multiple methods include Markus (above review) study on electronic mail and Eldabi et al. (2002) paper on decision making. These studies both show that quantitative data may be used to fund both quantitative and qualitative methods and to gain a richer understanding of the selected phenomena.

4.1.6 Inherited Issues and Problems

Reliability and validity are two constraints that any researcher must work with. Reliability relates to the internal consistence and credibility of measures in a research design and validity

relates to the external audit of claims against others who have done similar work and/or used similar research tools. Reliability is hence the accuracy metric match with the actuality of the phenomena under investigation. As the two can never be precisely simultaneously defined reliability is an estimate that will always incur error. The types of errors associated with reliability are systematic (that relates to the way the research was executed and consistencies in the context) and random (that accounts for natural and uncontrolled variation of for example the people involved). Hence reliability can be expressed as a ratio or percentage or a probability, and discussed in terms of consistency with expected values. A reliable study is one that conforms to expectations within the allowable margins of error and is repeatable by others within these margins of error. In a qualitative study consistency is found with repetition, in data triangulation, and matching rather than numerical representations. Reliability is hence more than a valid measure and is one that may be repeated consistently in the same conditions.

Validity is an external appraisal of the study that gives grounding to the study in relation to other completed studies. In a simple sense validity assesses the relevance of the study to the wider community of knowledge. It is possible to have a study that is reliable (internally consistent) but produces results that are wildly different from what is already known. The result can be interpreted in terms of new knowledge and a paradigm shift or in terms of incorrect objective setting for the study or unexplained errors in the execution. Validity hence provides a connection between the body of scientific knowledge and a particular study. The key contribution is in the audit of findings. In qualitative studies similar standards apply and validity is interpreted as a holistic appreciation of the approach, methodologies, methods, the execution, and adequacy of audit trails.

4.2 PRIOR RESEARCH

The review of literature in section 2 above identified freedoms for the researcher to choose from a range of different approaches to research. In IS there are many different approaches to research and many different ways of selecting methods. Theoretically and demonstrates by other researchers in the IS world no approaches, methods and mix of methods are excluded from possible research methodologies. In this section a range of issues, problems and topics of IS research are reviewed to observe how other established researchers have completed IS field studies. The reviews look at how the researcher approached the study and what methodological decisions they made to answer the research question.

4.2.1 Strategic Alignment

Luftman & Brier (2005, 1999) addressed both how IT is aligned with the business and how the business should be aligned with IT. They argued on organizations seem to find it difficult or impossible to harness the power of information technology for their own long-term benefit. Luftman & Brier (2005) used the survey data from executives who attended classes at IBM's advanced business institute, which represented over 500 enterprises in 15 industries. Luftman & Brier (2005) also used interviews and observations from consulting engagements. They identified the six most important enablers and inhibitors in the following order (see table 4.1).

Table 4.1: enablers and inhibitors alignment by Luftman & Brier (2005, 1999)

Enablers	Inhibitors
Senior executive support for IT	IT/Business lack close relationships
IT involve in strategy development	IT does not prioritize well
IT understands the business	IT fails to meet its commitments
Business/IT partnership	IT does not understand business
Well-prioritized IT project	Senior executives do not support IT
IT demonstrates leadership	IT management lacks leadership

In this study, Luftman & Brier (2005, 1999) asked the respondents to identify the enablers and inhibitors to achieving harmony between business and IT in their organizations. The executives were asked to rate the perceived strength of alignment with their organizations. Luftman & Brier (2005) pointed out that half believed that their business and IT strategies were properly aligned, 42% said they were not aligned, and 8% were unused or had no opinion. Within the context of their function (business or IT), Luftman & Brier (2005) asked the executives to identify the key enablers and inhibitors to achieving alignment in their organization. The notion that the respondent s' function area in business or IT would influence the ranking of enablers and inhibitors was also tested using the questionnaire data. Luftman & Brier (2005, 1999) claimed that analysis of the data showed significant similarities over the five-year span of the study in the perceived importance and raking of both enablers and inhibitors. The activities identified as enablers and inhibitors were comparable across industry and job title. In their conclusion, there is no single strategy or single combination of activities that will enable a enterprise to achieve and sustain alignment. Executives should concentrate on improving the relationships between the business and IT functional areas, working toward mutual cooperation and participation in strategy development, maintain executive support, and prioritizing projects more effectively.

A comparison of the IT alignment model to prior research identifies its unique contributions to the literature. Henderson & Venkatraman (1992) reviewed literature on the potential of IT to influence competitive advantage and found a lack of systematic frameworks to conceptualize the logic, scope, and patterns of organizational transformation that depend on IT. In response, they proposed the IT Alignment framework with propositions and management implications. The IT Alignment model is a framework for comparing, analyzing the IT department goals, objectives and activities to the goals, objectives and activities of the enterprise. The model developed by Henderson and Venkatraman (1992) shows: (1) IT strategy as distinct from IT infrastructure and processes; and (2) the concept of strategic alignment as distinct from bivariate fit (relationships involving two domains) and cross-domain alignment as a central element of organizational transformation.

Two other studies examined the social dimensions of alignment. Nelson and Cooprider (1996) found that mutual trust and mutual interest between IT and business people influenced their shared knowledge, which in turn affected IT performance. Subramani et al. (1999) defined a user gap as the difference between the user group's perspective on issues and the IT group's assessment of the user group's perspective. IT gaps were defined in a similar way. They found that both the IT and user gaps were inversely related to the operational as well as service performance of IT; however, the IT related gaps had a stronger effect on IT performance than the user gaps.

These studies differ in that their focus is mainly on the relationship between alignment and IT performance (Chan et al. 1997; Subramani et al. 1999), or between shared knowledge and IT performance (Nelson and Cooprider 1996). In contrast, other studies identify the factors that create or inhibit alignment. Another difference is that Nelson and Cooprider (1996) investigated the factors (mutual trust and interest) that lead to shared knowledge whereas other approaches do not investigate the antecedents of shared knowledge.

4.2.2 Social Alignment

Martin, et al. (2005) used qualitative research methods to study social processes of alignment in six government agencies. Their paper presents the results of a study of the social dimension of the alignment of business strategy with information systems and information technology. The social dimension of alignment, which includes mechanisms such as business planning style and business planning communication, is less well understood than the intellectual dimension, which includes audit, managerial reviews, and other traditional management accounting and reporting practices. The results show that the social dimension is

significant for alignment. Management support, with managers who cooperate in business and information system decision-making, and are literate in technical matters, is important. Their qualitative research methods included a 360 degree feedback mechanism for semi-structured and unstructured interview narratives and commentaries. Agency staff members were asked to provide views and personalised accounts of management support, business planning styles and business plan communications. The research method also used unstructured discussion and meta-story (that is, story about a story) techniques to develop a deeper understanding of individual perceptions, business group perspectives and life experiences. Archival research and document discovery and public announcements and statements by agency executives were also used in the research. As data were collected from multiple sources, triangulation of the data occurred similar to that in the research programs executed by Orden & Santos (2003).

Martin et al. (2005) asked twenty executives (CEOs, deputy CEOs, CFOs, CIOs and senior executive management) and 48 middle and junior managers to provide views and personal accounts on the social aspects of alignment. The reflective approach was aimed at developing comparable and balanced top down (executive) and bottom-up (staff) views of the social aspects of alignment under investigation, while also allowing researchers to identify differences in opinion and attitudes among the interviewed staff. They used interview commentaries, narratives and public statements and recorded in field note format, collated, transcribed and two-pass coded on to a purpose built research database using partial ordered display protocols as defined in Haughwout (2000). According to Martin et al. (2005), archival documents were analysed for evidentiary statements (for example, board meetings, executive management actions) using word, text and headings search techniques with the results integrated into the case analysis. Their research was conducted on the basis of agreed identity suppression, with the data and information collected in the period from December 2001 to October 2003. On their research findings indicated that, while public agencies viewed overt management support as important for the development of alignment, they also stressed the value of higher management understanding of the business and IS/IT issues, and the close business and IS/IT relationships that assist cohesive decision-making in the dynamic business environment.

4.2.3 IT Social Audit

Chowdhury & Chan (2005) used in-depth interviews with eight social workers used a decision support systems (DSS) in their work and from content analysis of narrative

justifications appended to 1,074 decisions that differed from those recommended by the DSS. They examined the thinking processes in the use of a decision support system (DSS) by social workers in a human services agency to determine whether they used the system to improve their case reasoning.

Chowdhury & Chan (2005) used a multifaceted qualitative research strategy with information obtained from content analysis of the social workers' narrative justifications and in-depth interviews. Their research findings also show, however, that the social workers used the DSS seriously under conditions of uncertainty. Under these conditions, they paid careful attention to the 80 questions that the DSS posed and found them a useful aid to thinking and reflection. The assumption of the DSS designers was that a discrepant recommendation would stimulate the social workers to rethink their own decisions. This is not what happened. The need to reflect was limited largely to atypical cases, in which knowing what to do was particularly difficult or in which the decision was particularly consequential.

The distinction between typical and atypical cases was an important data collection technique. Practitioners needed knowledge structures to make sense of what would otherwise be a bewildering cacophony of social stimuli. In typical cases practice wisdom, or tacit knowledge, provided the required structure and support case explication, through which the practitioner created a mental image of the case and shaped the unstructured and uninformed facts of the case into information that was meaningful for the task at hand. In atypical cases, however, case explication cannot be completed and a situation of uncertainty ensues. The findings suggested that the DSS helped the social workers structure and explicate atypical cases, in which they could not finalize these processes using their practice wisdom or tacit knowledge alone. In this way the research entered the abstract world of mental maps and participant explanations.

4.2.4 Network Relations

Beauprez (2002) used survey data to test a nomological network of relationships among factors that related to the organizational assimilation of Web technologies. They adopted a field survey methodology for their study. The unit of analysis was the enterprise with the assimilation of Web into e-commerce strategies and activities being the phenomenon of inquiry. In a pilot study, knowledgeable academics and practitioners reviewed the questionnaires. They used these reviews to ensure that their items unambiguously captured the appropriate constructs in their research model. Beauprez (2002) reported that 85% of the responses were received electronically. Their overall response rate was about 14%, with a

total of 75 pairs of responses being available for analyses. However, because of missing values, only 62 pairs of responses were used for analyses. The findings also had important implications for managers involved in efforts to introduce complex technologies such as Web technologies into their enterprises. The findings reinforced the importance of institutional factors such as top management advocacy, strategic investment rationale, and extent of coordination on the heightened levels of technology assimilation. These findings testify to the collective responsibility of senior management, business executives, and other executives in heightening their enterprises' technology assimilation success. While numerous advocates have prescribed such a collective responsibility as a normative guideline, the research provided empirical support for this prescription. Beyond senior management advocacy, they also demonstrate the importance of articulating an explicit investment rationale and implementing coordination mechanisms to facilitate the assimilation of Web technologies.

4.2.5 Technology Acceptance

Spacey, Gefen, Karahanna, & Straub (2003) investigated the attitudes of public library staff in the UK towards the Internet involved use of a mixture of quantitative and qualitative research methods. Their paper focused on the questionnaire survey used in the research and, specifically, discussed the use of the Technology Acceptance Model (TAM), which was adapted from Davis et al. (1989) to measure library staff attitudes towards the Internet. The research also involved qualitative focus groups, interviews and an online bulletin board with staff. This paper presents selected results of the questionnaire survey and reflects on the appropriateness of the TAM for the study.

The aim of the survey was to generate sufficient data to piece together a picture of public library staff attitudes to the Internet. Gathering the views of as many staff as possible was considered advantageous and surveys were regarded as the most appropriate method to achieve this since they can generate great amounts of quantitative data from large numbers of respondents. In relation to the aims and objectives of the study, questionnaires can also be useful in discovering both facts and opinions such as attitudes. Furthermore, a self-administered questionnaire is a cost effective method of questioning a large number of people, being relatively easy to administer. They are flexible in that they can be used to collect a wide variety of data in a variety of different circumstances.

Several draft versions of the survey were deliberated on and the staff of a central library tested an acceptable version of the pilot during early 2002. A number of amendments were subsequently made to the survey in order to improve its overall appearance and

relevance to public library staff. Some respondents had noted that they demonstrated the Internet to customers rather than using it themselves and the manager of the library participating in the pilot study. Hence a question relating to staff feelings about assisting the public in their use of the Internet was included in the actual questionnaire. The survey was designed to establish facts about respondents including demographic and organisational variables, attitudes towards use of the Internet at work and opinions of a wide range of training methods for use of the Internet. Survey data could then be used for statistical analysis using the Statistical Package for the Social Sciences (SPSS) to consider the influences on attitudes.

4.2.6 Evaluating IT Value

Yoon & Im (2005) present an evaluation framework for IT outsourcing customer satisfaction through specific literature reviews and expert interviews, and develop an IT outsourcing customer satisfaction evaluation system using Analytic Hierarchy Process (AHP) analysis. Their paper aimed to introduce a systematic evaluation system for the evaluation of IT outsourcing customer satisfaction that reflected outsourcing environments as well as customer feedback. AHP was used for weighting and ranking key customer satisfaction factors. The system was applied to IT outsourcing customer companies in Korea in order to demonstrate the practical value and effectiveness of the proposed system. This study may be useful and helpful to practitioners, IT managers, and customers who are faced with outsourcing services. Using the evaluation system as a tool for measuring IT outsourcing customer satisfaction, IT outsourcing providers can monitor their service level and precisely understand customers' requirements. The observed values of customer satisfaction can provide important guidelines in the improvement of IT outsourcing services and improve their competitive position in the market. For customers, they can utilize the results of customer satisfaction in choosing IT outsourcing vendors.

Information technology outsourcing, customer satisfaction, and a related information system evaluation model was reviewed in the second section. They developed an evaluation framework for IT outsourcing customer satisfaction using the AHP applications. They reviewed the related literature and extracted key elements or factors that had an effect on customer satisfaction in IT outsourcing environments. They conducted interviews with nine IT outsourcing experts who were related to the IT outsourcing service industry, academia, and government in order to generate customer satisfaction-affecting factors and to verify extracted key factors from the literature reviews; then they defined all customer satisfaction-

affecting factors. Subsequently, they constructed an evaluation framework for IT outsourcing customer satisfaction, which was classified into consulting service satisfaction, customer supporting service satisfaction, and performance satisfaction.

In their survey, IT outsourcing services were classified into five areas: Application Service Provider, Hosting and Data Center Operations, Application Development and Maintenance, System Operations and Support, and an Outsourcing Hybrid based on the classifications of IT outsourcing service. They sent 120 questionnaires to 40 customer companies that outsource IT functions. A total of 25 companies from the five outsourcing areas participated in the survey. They received 32 usable and meaningful responses, and an overall response rate of 27% through the questionnaires. They viewed the evaluation system as a useful tool to monitor or manage IT outsourcing companies' service level and understand customers' requirements precisely. By using the tool, IT outsourcing providers could evaluate their customer satisfaction levels by themselves and give customers a high degree of satisfaction. They could also utilize the weights of the customer satisfaction factors to improve the outsourcing services quality. From the viewpoint of customers, enterprises can utilize the evaluation system in choosing IT outsourcing vendors or deciding the level of IT outsourcing.

4.2.7 Researcher Preferences

IS research is broad in its approaches and is inclusive of a comprehensive range of methods. The best explanation for these observations are found in various IS Journal articles that refer to IS as a reference discipline for others (Barnes, 2005) and also a discipline that draws on other disciplines (Basketville & Myers, 2002). The former is a position that is argued for in more recent publications. These articles attempt to explicate IS studies from claims that IS is simply a parasite living off the academic credibility of other fields of study, such as, computer science, engineering, psychology and so on (Katerattanakul et al., 2006). The criteria and standards that are used to select papers for the top IS Journals (for example MISQ) are held as indicative of independence amongst academic fields. However, irrespective of the sides in this debate IS research accepts a wide and diverse range of approaches. The choices for a researcher are open and can be guided by what others have done before but also managed in ways that best suit the research questions and researcher perception of problems in the field.

In the IS literature reviewed in sections 2 and 3 above the concept of a hybrid approach has appeal in conditions where there may or may not be access to the required data

and the response rates may be low. In the area of IS security it is anticipated access to protected business data will be impossible and the expected levels of disclosure will be low. In addition previous studies (see Section 6.1.1) have shown that response rates in workplaces are generally low unless a participant is authorised by a superior to respond. In section 3 it is clear that a wide range of topics are addressed in IS studies and the studies have a diverse data range. The most frequent data collection techniques were questionnaire and observation, and the most frequent method was survey. The research on approaches showed that quantitative approaches have dominated IS research up until the late 1990s but that an increasing number of qualitative approaches have been apparent in the 2000s. The arguments against a more than one-shot one-run statistical survey have been adopted in contemporary IS studies (as reviewed above). The IS community expects a comprehensive range of data that informs a holistic view of IS and address key issues. Hence researcher preferences ought to consider the changes in the IS field, the nature and importance of IS in enterprise systems, and the expected outcomes from an IS study.

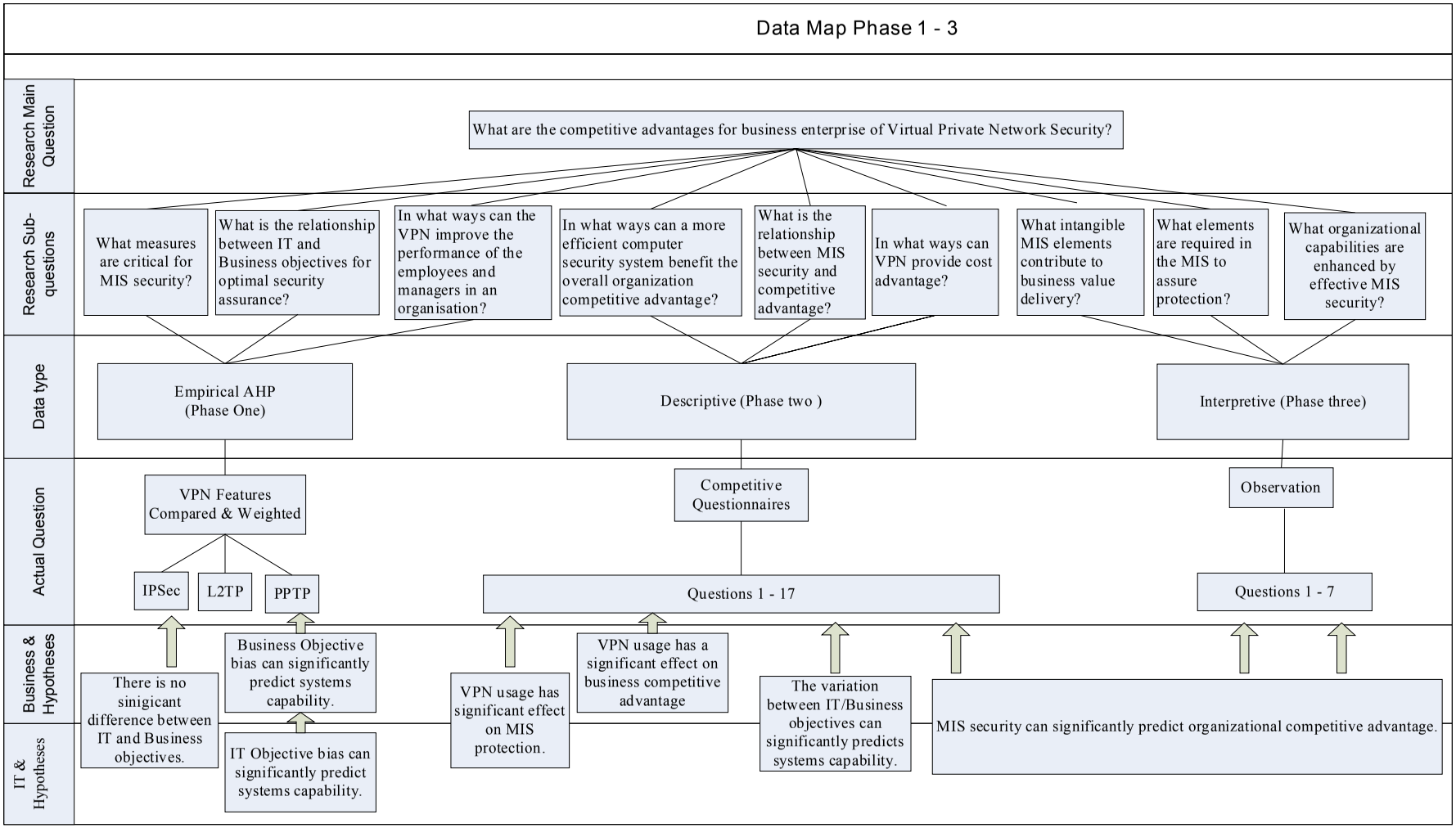

Figure 4.3: Data Map

4.3 THE PREFERRED RESEARCH APPROACH

The literature reviewed in this Chapter addresses a number of issues that have confronted other researchers and the literature also elaborated solutions they have applied. A clear message is that the approaches to IS research have broadened over the last fifteen years to embrace mixed methods, hybrid approaches and qualitative studies. The foreseeable constraints on a plausible data field and the forecasted sample sizes (as per other researcher experience and quoted in Section 4.1.1) lead the researcher to expect difficulties in a one shot quantitative study in this proposed investigation. The literature would suggest that in an organisational context, interacting factors will mitigate any measured effect and that filters (variable conditioning) would be unlikely to sufficiently condition the range of uncontrolled variables. This is particularly relevant in business and dynamic areas of organisation cultures. The likehood of erroneous findings in such conditions is high and yet the reviewed literature suggests that hybrid methods provide a solution where interaction may be explained in a network of several data types.

Consequently, the preferred research approach will be a hybrid model that retains a quantitative perspective but also relies heavily on qualitative data to provide evidence for hypothesis testing and justifying asserted claims. The Markus reference study (reviewed in Section 2.4) provides a framework to guide such an approach. In addition the researcher can systematicaly define variations and control research effects by taking instruction from the other researchers reviewed. The approach hence allows the use of different data collection techniques and data analysis strategies. However, the researcher prefers to quantify data and to qualify claims. This is the debate raised in Section 4.2.0 where the statistical analysis must address the subtantative issues of the field context.

A weakness in this preferred hybrid approach is that the line between statistical inference and subtantative justification is blurred and open to interpretation. The weakness is a risk the researcher expects to manage by triangulating data types and by seeking trust in data analysis tools validated by others in other studies (for example, AHP and Likert tools). The findings themselves will be compromised unless the researcher can triangulate the statistical outputs and develop coherent grounds for truth claims. The approach is not new but adaptable to different IS research contexts. A central issue is the development of metrics and the validation of findings. This impinges on the extent to which research findings can be transferred or generalised. Hence the extent to which the researcher can provide a comprehensive coverage of the data type and the reliability of the data collection tools is critical. The effectiveness of the field research and its validity in the hybrid approach do not rest on one particular method. Hence variation is allowable

in the precision of any particular measure and the variation may be explained using a non quantitative data type. For example, a statistical output may be judged erronous by contextual interpretative data and the explanation integrated into the network of findings that justify truth claims. Again the preferred approach may be challenged by purists but it may also be defended by pragmatists and the cases published in prior IS research.

My investigative interests in research methods led to the use of triangulation methods. Triangulation is the application and combination of several research methodologies in the study of the same phenomenon. It can be employed in both quantitative (validation) and qualitative (inquiry) studies. Triangulation method is preferred in the social sciences due to its strengthens to combining multiple observers, theories, methods, and empirical materials in which Sociologists hope to overcome the weakness or intrinsic biases and the problems that come from single method, single-observer, single-theory studies. In the research method literature reviewed, mixed method designs can yield richer, more valid, and more reliable findings in particular contexts that are similar to the proposed research field, than evaluations based on either the qualitative or quantitative method alone. A further advantage is that a mixed method approach is likely to increase the acceptance of findings and conclusions by the diverse groups that have a stake in the evaluation. Figure 4.1 summarises the dynamics of the preferred approach by linking the hierarchical divisions that cross large organisations (see Section 4.1.2) to the triangulation of data type. The respondents (to the structured questions and the observations) are clustered into IT and into business roles. Triangulation can filter the respondent perspectives and allow auditing of competing and complementary claims. The output of the triangulation process can then provide networks of information that can be used as primary data for the testing of hypothesis, answering questions, and asserting justified claims as to best practice in information security.

4.4 RESEARCH DESIGN

Figure 4.1 provides an outline in which the dynamics of the proposed research can be conceptualised. VPN has been characterised as an organisational cultural artefact (see Section 4.2.6) that provides a link between the IT business infra-structures and the organisation business structures. VPN is a visible connection between these two worlds in enterprise systems and facilitates interaction in ways that have potential for mutually beneficial business outcomes. VPN has particular features (see Section 2.3) and services (see Section 2.3.1 - 4) that inter-relate with the business expectations and IT objectives. VPN consequently is an object for study and the properties of VPN provide the necessary problematic relationships for investigation. Figure 4.1 depicts the contextual situation of

mutually exclusive IT and business worlds but introduces the method of triangulation as a way of seeing the two worlds interacting from three independent perspectives. Once triangulated a network of business and IT information is established that has independent components and also inter-related comparative information. The networked information can then provide sufficient grounds to justify statements (within the limits of the methodological framework) and necessary conditions for making decisions, such as hypothesis tests. The dynamic conceptualisation of probable researchable relationships hence leads to possible statements about protected MIS and its characteristics.

The dynamic conceptualisation of the research leads to a static visualisation of the research problem. VPN is positioned at a critical interface within enterprise systems. It supports work systems and provides a level of system security that both IT and business people trust. VPN capability is trusted to deliver protected business information. The work systems of an enterprise are implicated in the attainment of organisational goals and by association VPN is implicated in goal delivery at the objectives level. The importance of VPN is that it is implementing both business performance and IT attainment objectives simultaneously. Hence, the study of VPN in context is ambiguous and is best studied as a dynamic enterprise system element. However, as a static visualisation VPN can be seen as an interfacing object caught between IT compliance and attainment objectives, and business performance objectives. Figure 4.3 captures the sense that a VPN is in an interstice of trade-offs that provide both meaning and value for the object. The figure is indebted to Steven Alter's long standing analysis of work systems and their place in enterprise systems. The definitives added to each face of the cube are lifted from Alter (1999) to enhance the visual complexity of the conceptualisation (Extracts from Porter's work could equally be added to the competitive advantage face). There is no intention to suggest that a VPN can be represented by a line, a curve or a surface within the cube but rather that any element or aspect of a VPN is open for interpretation from many different perspectives, each with different adjudication values, and with different expectations. VPN in this sense is no longer an entity owned and defined by an IT perspective, but rather an organisational cultural artefact and object that may be investigated from many different perspectives.

Figure 4.3 also introduces the notion that observation and investigation in an enterprise context occurs with a diverse data range. In this instance three feasible data type are defined as empirical, descriptive and interpretative. The data types cohere with the organisational phenomena of security expectations, competitive advantage and work systems. These associations and untested assumptions provide a framework in which the research problem can be conceptualised. As it was defined in Figure 4.4, the research question may be divided into logical sub-questions that are grouped (in threes) according

to data type. The organisational context is hence interpreted to be of a grounded empirical nature as associated with matters of security knowledge, of a descriptive type as associated with claimed competitive advantages and of an interpretative type as associated with the more volatile and ambiguous work systems data. As a conceptual model it is helpful to visualise these elements intersecting and interacting in the cubic space and the important relationships for research being defined in a negotiated context. The hypothesis assert (see Section 4.0) the range of beliefs derived from literature and they may be tested within this context.

4.4.1 Data Sample

The selection of a data sample is a critical element in the operationalisation of the research objectives. The sample is the opportunity for a window on the real world and also a limiting factor in what may be claimed or transferred from the study. The sample consequently has to be justified in terms of what is expected (from the theoretical readings above) and what may be achieved in real terms. In the following sub-sections the realities of field work are discussed in detail to define a prescription for data collection that optimises the various trade-offs. First the issue of response rates and the New Zealand business context are discussed to identify limitations on the scope of a study. Second the organisational structures in which business and IT are done are revisited and a representative sample defined. Third international differences are discussed to identify issues and potential problem areas that would need managing for international data collection. Fourth the worlds of IT and business are reassessed to identify an opportunity sample. And finally, each of these components are put together in a working solution for an optimal and feasible theoretical sampling strategy.

4.4.1.1 Field limitations

Access to businesses for data collection is always difficult and the most successful researchers (for example, Fielden 2004) build up a relationship over an extended number of years. The long term researcher relationship builds trust and understanding of the risks faced by both parties. To the contrary, short term relationships return a 14% response rate (see section 3.4). Disclosure is a major issue that has to be negotiated between the researcher and the organisation. In the area of security most organisations prevent disclosure with a blanket protection of any information in relation to the security systems and its layers. It is also important that the researcher can act with independence so the data collected is sufficient to answer the research questions and has minimal bias.

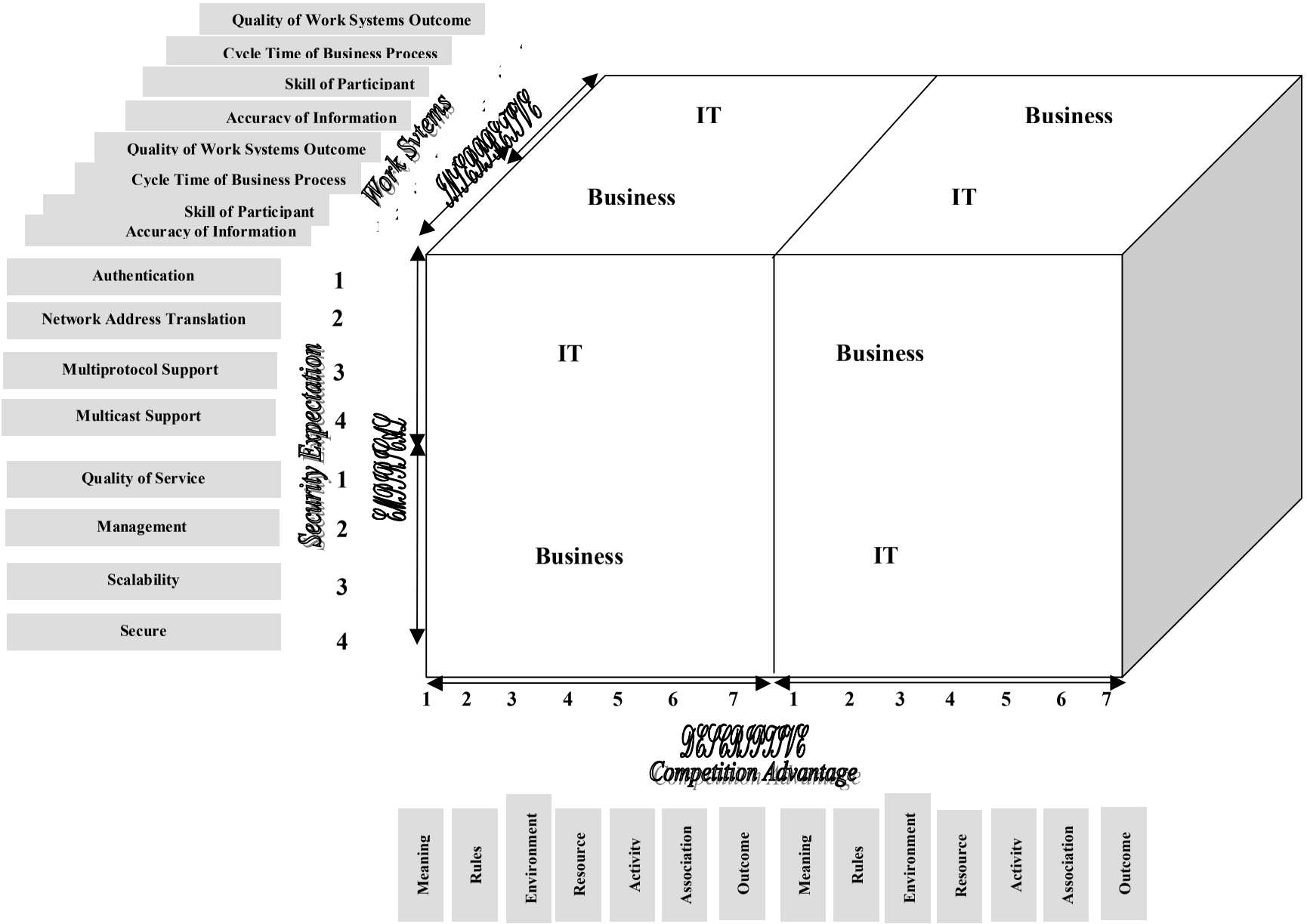

Figure 4.4: Static Visual Cube: VPN Interstice & Systems Expectations

Online questionnaires have a unique problem set, namely: complete responders, unit responders (did not participate at all), answering drop-outs, viewed but did not answer questions, viewed some but not all of the survey, item non-responders (only answered some of the questions, but completed the survey), and item non-responding drop-outs (answered some questions, but dropped out before completing). A lack of survey salience (the association of importance and/or timeliness with a specific topic to a potential survey subject can also reduce responses (Nonnecke, 2000). Response rates may also be affected by some systematic judgement by a segment of the population being studied, causing them to be excluded from the result (Paolo, et al., 2000). For example, invitations to participate posted on discussion groups may get higher response rates from technical discussion groups because they are more interested in any type of online interaction while those groups dedicated to health support issues may interpret the survey participation request as an intrusion on their privacy (Paolo et al., 2000). The attrition rate, the number of people who started to take the survey, but did not complete it can be used to reveal some systematic judgement by a group (Taylor, 2000). For example, attrition rates may be calculated if the survey captures the link-to source of the survey. Counts by that source for completed and partially completed surveys provide the basis for rate calculations. Another reason for high non-response rates may revolve around issues of privacy and confidentiality (Tuten, et al., 2000).

In the literature review, several studies show that web-base surveys produce a significantly lower response rate than traditional mail surveys (Birnbaum, 2004; Truell, 2003). One study indicated no significant differences between the two methodologies. Researchers doing studies using web-based surveys have also found lower response rates than for traditional mail surveys (Griffis, 2003). However, unless the web-based survey uses a sampling method that allows only certain individuals to access to survey, it is impossible to know the response rates. For example, when participants for electronic surveys are recruited via newsgroups, search engines, or electronic mailing lists, researchers are not able to pinpoint the number of individuals who received the information, and therefore they cannot determine response rates nor speak to the representative ness of the sample (Vermaas & Wijngaert, 2005). To circumvent this difficulty, many web-based surveys make use of an initial e-mail to a targeted group that contains a specific URL to access the survey. This e-mail can also include password to ensure that only those who have been targeted can complete the survey and to prevent any individual from completing the survey more than once. However, researchers are cautioned not to make the web-based survey too difficult to access by requiring too many codes and passwords, because this added complexity can lower response rates.

Another design feature that seems to affect attrition rates is the location of the request for personal (demographic) data in the survey. Attrition rates were significantly lower when personal data was requested at the beginning of Web-based survey rather than at the end of the survey (Nonnecke & Preece, 2000). Placing the data request at the end of the survey presents a surprise to the respondent to which he/she reacts negatively by dropping the survey before completing it. Placing the data request at the beginning may be perceived as honesty on the part of the researcher. This helps to create an atmosphere of greater trust and to build a quality relationship. How survey subjects are invited to participate in the survey, and how survey completion is encouraged through reminders, can affect response rates. The perceptions of burden (the effort required to complete the survey) can be manipulated and affect non-response and attrition rates (Andrews, et al., 2001). For example, those who were told the survey would take less time, those received an automated (embedded) password, and those who received more frequent reminders, were all more likely to accept the invitation. However, these factors did not have significant effects on signing up for the survey (Birnbaum, 2000). The use of automatically generated passwords in email invitations to protect against "ballot stuffing" and allow subjects to break off and re-enter to complete a survey can affect attrition and non-response rates. When subjects were given passwords having no ambiguous characters their response rates were significantly higher than those subjects with password ambiguities (Couper, 2000).

Technical difficulties can be encountered while sending the questionnaires online to respondents. According to McCoy & Marks (2001), technical difficulties alone may keep response rates low. Problems of sending and receiving questionnaires online via internet including compatibility of server formats, non-transferability of word processing codes, and the inability of less computer literate online user to download and upload the questionnaire, a more particular approach was taken. The implication is that an electronic approach to data collection may be unsuitable in circumstances where an incentive is needed to ensure high response rates. For this particular research, the inclusion of an incentive was unnecessary, so the problem did not arise. Another concern relates to the difficulty in incorporating high quality images or colour within the questionnaire. It is certainly true that researchers who use a simple e-mail approach have relatively little control over how the research instrument appears on a recipient's machine.

Some respondents e-mail disable confirmation of receipt and reading software so this option may not obviate the requirement for a country-based batch approach in questionnaire online. Author tried to avoid sending or contact respondents on the weekends because working hours. This research found the on-screen appearance of the questionnaire at the point of response cannot be guaranteed in the way that a mailed

questionnaire can. Using a web page helps considerably, but more comprehensive testing of the questionnaire using a variety of different browsers may be appropriate identifying respondents: it is preferable to tag respondents with some kind of identifier as, in theory, an individual can visit the website and answer the questionnaire on many occasions expediting data input: the possibilities of data input errors can be reduce and time saved by linking respondent's replies directly to a spreadsheet or other data capture software.

The sample opportunity is also limited by context. According to the New Zealand (NZ) Ministry of Economic Development (MED) website (http://www.med.govt.nz/) businesses in NZ may be grouped into the following clusters for analysis:

- Zero employees
- 1-5 employees
- 6-19 employees
- 20-49 employees
- 50-99 employees
- 100-499 employees
- 500 or more employees

The statistical analysis then shows that:

- 96.3% of enterprises employ 19 or fewer people.
- 86.5% of enterprises employ 5 or fewer people.
- 63.2% of enterprises have no employees.

The implications for research are that few businesses (.09% See Figure 4.5) are large in employee number.

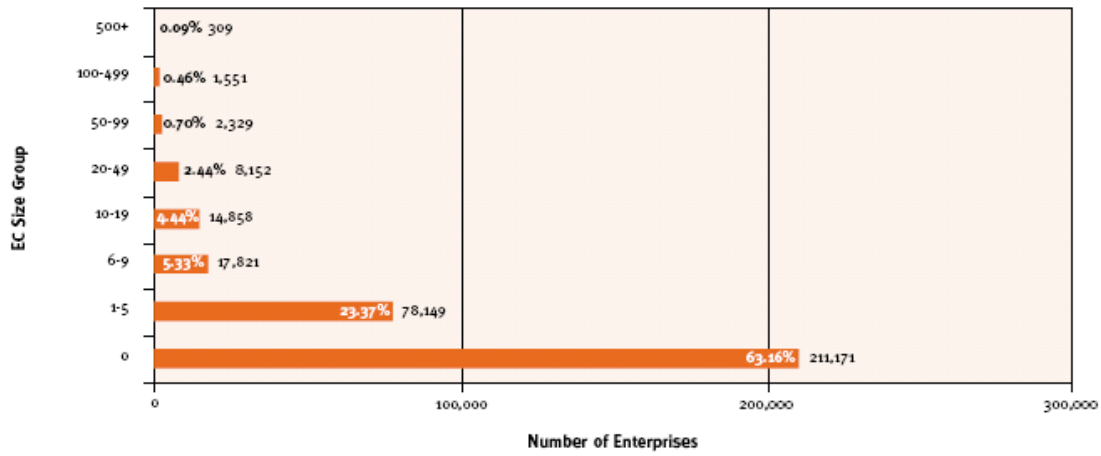

Figure 4.5: Number of Enterprises by Size, as at February 04

Further useful analysis shows that more large businesses are in the private sector than the government sector, and the universities are classed as large businesses.

Table 4.2: Private and Government Sector Enterprises by Size, as at February 04

	Number of Enterprises	
EC Size Group	Private Sector	Government Sector
0	210,899	272
1-5	77,756	393
6-9	17,348	473
10-19	14,145	713
20-49	7,317	835
50-99	2,056	273
100-499	1,311	240
500+	215	94

Other measures can also be of use in selecting enterprise systems for study, for example turn over, annual profits and so on. However, the NZMED data provides a general indication that the availability of potential study sites by size and the IT intensity is limited in NZ. A further consideration is that the majority of medium and large business are foreign owned or have a substantial foreign ownership. Most of these enterprises report to head offices overseas.

A further consideration in identifying limitations imposed by the context for a field study is the expected response rate from a speculative sample. The majority of people projected to be of value in a study of VPN usage are people who are focused within business systems. They are time scarce and work with excessive demands. The expectation for responses within this context would be marginal. Previous research shows that 14 - 30% response rates can be expected with different media and international jurisdictions (see section 3.4). In NZ the reported response rates are even lower, for example Fielder (2001) 18% and Nicho (2004) 12% in survey research. These figures indicate that simple surveys and distributed questionnaires may not be sufficient to gain the depth and range of data required to answer the research question. The NZMED data (quoted above) also suggests that gaining sufficient data within NZ businesses would also be a difficult undertaking.

4.4.1.2 Organisation Structures

Large enterprise systems tend to organise themselves in similar ways and then continually evolve for competitive advantages (see Sections 2 & 3 for elaboration). These structures divide an enterprise into units for accountability, management and performance reasons. Variations occur for competitive advantage but the size of variation tends to minimise in large organisations. The definition of a large organisation in the NZMED terms includes 309 possible enterprises (see data quoted above). In international comparisons the number of large enterprises reduces to 15 – 20. Standardisation is greater in larger organisations and role based behaviour sanctioned within tight expectations. As a consequence

collecting data within large organisations can be conditioned by the nature of the organisation itself. Organisational conditioning can filter uncontrolled variables that arise from personal agendas, the organisation structure (ie. compared with smaller enterprises with wide variation), role performance, IT expectations, and business expectations. Such conditioning can provide controls for the data and enhance its value. However, the dynamic and fluid context of enterprise systems prevents the experimental design being reduced to the interaction between two variables. All variables within the enterprise system experience noise from the interaction of many variables within the context. Organisational structure hence is a filter that helps a researcher control variables in a dynamic context and to locate problems in a semi-conditioned space.

4.4.1.3 International Differences

International differences are found in the legal, the political and the cultural layers of enterprise systems. Particular differences are found in the role designations and the decision-making powers within different enterprise systems. For example, in NZ the top executive leadership role is usually a CEO (Chief Executive Officer), and the CEO has immediate recourse to other chief titles (the "Cs") such as the CFO (the Chief Financial Officer), the CIO (the Chief Information Officer) and so on. In the US the top role title is usually the President and the president has immediate recourse to Vice- Presidents of various functional descriptions. Size also influences the number and type of titles within any enterprise structures. For example, a small enterprise may have a managing director as the head role in NZ and a large one a suit of Cs. As a consequence differences are found between different geographical jurisdictions and even within the same brand in different jurisdictions. However, the extent of difference is minimised (but not extinguished) the larger the enterprise system. In any study that attempts to generalise across international boundaries a discussion and recognition of differences is necessary. Quantitative approaches must explain differences and qualitative approaches require rich data and case analysis.

4.4.1.4 IT / Business Perspectives

The alignment issue has been discussed in Chapter 3. It was established that IT and business have different ways of executing higher level objectives at the tactical and operational levels. These differences are supported in the IS literature on alignment. Alignment is construed to be a strategic problem that has strategic consequences for the enterprise system. It was not enough to declare that business people specify the business objectives and the IT people do them. The concept of alignment required that the differences be acknowledged as different perspectives within the one enterprise system

and that the complexity of the relationship between the two different perspectives planned for through strategic alignment (for example, Henderson et al. 1993, domain-pivot-target strategy). The implications for field studies of these observations in the IS literature is that the field is divided into strata. Consequently a good theoretical sample would include sampling within each strata.

4.4.1.5 A Theoretical Sample

An ideal sampling methodology would be a cost effective one that randomly selects a representative sample of the population parameters within an allowable margin of error. And further the ideal sample would have minimal error so that the statistics accurately predict the population variables. However, the preceding subsections indicate that there will be many problems in the theoretically available field. In sub-section 6.1.1 identifies the problems other researchers have experienced with response rates in the sample space, and the statistical analysis of NZ businesses that leave very few entities to approach in the internationally large group. Sub sub-section 6.1.2 identifies the issue of organisational difference. It appears that large business organisations have less variation and therefore present a semi-conditioned sample for case analysis. Sub sub-section 6.1.3 identifies international differences as being a factor in the selection of a sample. A NZ sample for example reflects the legal, political and cultural constraints of the NZ business context and may limit the transfer of findings to other business contexts. Sub sub-section 6.1.4 identifies strata within any enterprise system that divides the business and IT interests into two distinct domains. In one instance the business interests are setting business objectives for the enterprise and in another the IT people have to interpret the objectives into a different knowledge domain.

The constraints summarised in each Sub sub-section influence the selection of a field data sample. An economic sample is critical within the project resource constraints. Data access is also a critical constraint in the security study area. Ideally a random stratified sample would predict the best quantitative outcomes. However, the real possibility of rejection of access to the required data and the non-response levels, require management and consideration of the pragmatic field trade-offs. The adoption of a hybrid research design (as discussed in as discussed in Section 2.4 above) provides possibility to mitigate the risk involved in a purely quantitative approach. The data range can be diversified and triangulation used to audit data against reliability benchmarks.

The issue of sample size can be addressed by recourse to discussions of power function (for example, Hair et al., 2001, pp. 10 – 13.) and then by interpretation of these quantitative considerations into the hybrid model context. The power function provides a quantitative researcher with a way of balancing the significance of a study with inferences

that may be made in the substantive world from the statistics. In the ideal world every study is a census but in reality every study is a sample from which inferences are made regarding the population. Consequently a power function balances the reality of sample with the necessity of declaring truth and the variation of evidence from the population truth. The discussions above, in the Sub sub-sections has located a number of potential differences between a perfect sample and the reality of field data collection. The power function can mitigate the acceptability of error (the false positive) with the identification of statistical significance when it is present. The calculation is based on the required effect size, the acceptability of error (as above), and the sample size. In a purely quantitative study these three factors may be specified to deliver an ideal power measure that can define the value of the study. In a mixed methods approach (hybrid model) similar trade-offs can be adopted to express the required level of acceptability of a study. Hair (2001, p. 13) suggests that a power function of .8 and the ambition of a .35 effect size is a strong starting position for a field study. To achieve this power a choice of acceptability measure and sample size may be made. In the proposed hybrid model consideration is required of the variability introduced by the range of data type and their treatment. Hence a reasoned interpretation would be to minimise the acceptability error while keeping the study size economically small as possible. The sample size must also keep in mind the possibility of non-responses and the influence on the power.

A theoretical sample, that reflects consideration of each of the discussed constraints would then include the international difference, the strata within organisations, the size of organisations, the aim to achieve a recommended effect, and the desire to minimise error. Hence a plausible sample would include large organisations (turnover > us$1 billion per annum, and >500 employees), the location of these organisations in three different international jurisdictions (for case triangulation audit), the selection of a sample size of 120 (as per a power function constructed from the above discussion of constraints and the divisibility into 3 x 40 (international locations); plus the 40 into 2 x 20 (business & IT strata). Alpha = 5%), and the division of sample into business and IT strata. These measures would balance the potential risks against the economic viability of the study. A lower alpha would involve a sample of 190 but this would be more expensive and more difficult to obtain. A higher alpha would reduce the number of participants required but increase the potential for error. Overall the reasoned adoption of this proposed theoretical sample optimises the perceived constraints in the probable data field and allows for the expected variations. The enhanced data range mitigates the quantitative risk of reducing the power to an unacceptable level (say below .7) on account of low response rates.

4.4.2 Data Types

Data type may be differentiated by the characteristic exhibited at the time of collection (as discussed in Section 2 above). The sub-sections below define the characteristics of different data type and the collection tools that best relate to the type. The three data type that are anticipated to be encountered in the field work are empirical, descriptive and interpretative. Data type is distinct from (but related as a property of) methodological approaches of the same name.

4.4.2.1 Empirical

Empirical data are collected with the use of questionnaires or structured tools as are found in the natural sciences. The empirical data the tools collect comes from the observations and experience of the participants. In the IS literature (reviewed in Section 3 above) observation and experience are elements of the research space and valid data to collect. Unlike the natural sciences where empirical data are fundamental natural elements, the IS literature is concerned with actual events, processes, or phenomena that occur within the information space. The theories used to explain the elements of the research space are independent entities that may be judged (effectiveness criteria) on the ability to adequately explain the elements concerned. In this way different theories may be used in the natural sciences and IS, and also within any preferred domain of inquiry.

4.4.2.2 Descriptive

Descriptive data can come from questionnaires but in the proposed study observation is also a source of descriptive data. The capability to describe configurations and human behaviour adds significant information and knowledge to the study context. Descriptive data may appear as text, recorded interviews, grouped numerical data, images, relational maps, and other networks (see Section 2.2 above). The data may be stored in tables and archives for ready access. The distinctive property of descriptive data is its rich and networked relation to the context and other data sets. It describes a situation and the related elements but cannot be used to establish causal relations.

4.4.2.3 Interpretative

Interpretative data acknowledges the mediating influence of theories and the phenomena in a study. Interpretative data is found in the abstraction from reality and within the preferred framework for explanation. Unlike empirical data interpretative data need not have a material reality and can exist as only a speculation or an untested abstraction. The data is distanced from the phenomena and mediated by researcher preferences (see Section 2.3 above) and yet carries explanatory power associated with a preferred position.

In this proposed field study interpretative data can assist the explanation of human behaviour and VPN usage.

4.4.3 Data Collection

Three ways of collecting data are proposed that are in keeping with the hybrid approach and the data type specification. Questionnaires, observation and unstructured interview are proposed. In the following sub-sections use tools and its validation are specified. The questionnaires are found in Appendix 1 and the data map in Figure 4.2.

4.4.3.1 The Pilot Study

The questionnaires are to be constructed from CISCO, Microsoft and other industry survey instruments. Individual questions are to be selected for the relevancy and potential for answering the research question (see data map Figure 4.3) and then compiled into a survey instrument. The questionnaires are to be available online or in hard copy for the participants. Hence a pilot study is required to test the reliability and useability of the constructs. For this purpose an equal sample of business and IT experts – 14 in total will be chosen to provide feedback. The feedback is to be processed as beneficial opportunity sample data and hence the researcher will moderate and act on the suggestions that are made. Three states will be accepted: Single, Multiple, Conflicting. Weightings shall be given of 1, 2, and zero, and the tallies compiled so that the highest number is the most urgent action. Negative and positive responses shall be treated independently so that the same item may receive a strong positive and a strong negative but the numerical weighting can highlight a property that requires action. The actions are: include, exclude, and modify.

4.4.3.2 Questionnaire 1

The purpose of the first survey is to collect empirical data (see Sub sub-section 6.2.1) from the user's and the IT managers of VPN systems. The construct starts with the definition of VPN properties (see Section 2.3) and the generation of questions in keeping with the research sub-questions. The two CISCO service papers were also reviewed for VPN properties and user attributes ("MPLS-Based VPNS: What's Possible for Enterprises" (2005), and "Managed IP VPN Services For Enterprise Organisations" (2005)). The Microsoft white paper (2003) "Virtual private Networking with Windows Server 2003: Interoperability", was reviewed for protocol definition and customer interfacing properties. The questions were then trialled in the pilot study and amended (see section 6.3.1). The questionnaire is in Appendix 1.

4.4.3.3 Questionnaire 2

The purpose of the second survey is to collect descriptive data on the relationship between security (VPN usage) and competitive advantage perceptions. The motivation for this question set came from Alter's (1999) work on work systems, Porter's (2001) work on competitive advantage, and Luftman's research on IT and competitive advantage (see section 3.1, & prior). The data set is descriptive as the target data is speculation on the part of the participants rather than concrete empirical evidence that may come from experience. The connection the respondents make is between their conception of competitive properties and the usage of VPN. Consequently the questions are starters (and in fact are not complete questions) that identify critical edges of business and IT objects. The users are asked to respond on a Likert scale of 1 to 5 so that a weighted impression of their perceptions can be gained. The questions were then trialled in the pilot study and amended (see section 6.3.1). The questionnaire is in Appendix 1.

4.4.3.4 Observations

While the VPN users are working simple leading questions will be asked to have them talk about what they are doing, why they are doing it in a particular fashion and how they construct the action. The purpose of the unstructured interviews is to co-ordinate actions with the users thinking, and to explore the user mental map within a work system. To a large extent this data is interpretative (see section 6.2.3) but useful for exploring the context of VPN usage more fully. The researcher is to sit to the left, slightly behind the user, and at the same level so that the field of work is not obstructed or imposed upon by the researcher, and yet visible. The visibility is for the work surface rather than the user facial and eye movements. The questioning hence enters the space as an abstract and rightfully elicits abstract responses from the user thinking. The observer will not use hand or body movements nor attract attention away from the work surface.

4.4.4 Data Analysis

The data analysis is to occur once the data has been collected. No uncontrolled feedback loops will be used to feed data back to participants for additional responses, and the researcher will not act on any of the data to change behaviour or actions in the field. In this way the data is to be collected according to the prescribed plan laid out in Sections 6.1 – 6.3 above and in keeping with the overall research design. In the following sections the three levels of analysis are to be defined. First all data is to be inspected for relationships, including international variation. Second the data is to be split into IT responses and Business responses, and the separate grouped data inspected for relationships. Finally the data sources (and types) are to be triangulated to identify

relationships that are common or missing from the individual data type data analysis. In this way the analysis can be exhaustive and extract the greatest number of possible relationships that may contribute to answering the research questions.

4.4.4.1 The Overview

The collection of data is made using three different methods corresponding to the three data type. The types are Empirical (collected using the AHP method for VPN protocol data), Interpretive (collected by observation and questioning of workers for Business work system data), and Descriptive (collected by survey for business competitive advantage data). The reliability can be tested by triangulation and type consistency. The distinct types and methods are to be analysed separately and then triangulated to collect any additional exception data.

In this research project the data is coming from a number of different places at different times. Hence procedures are set up to log the information in a database and to keep track of it until the researcher is ready to do a comprehensive data analysis. In this case, Microsoft Access is to be used, and it is to be structured (forms and alerts) which can be assessed at any time shows what data was already in and what is still outstanding. The data analyst should always be able to trace a result from an entry back to the original forms on which the data was collected. A database for logging incoming data is a critical component in good research record-keeping.

The overview data analysis takes all the data regardless of divisions within the sample and reports the research findings. In the first instance (phase 1), the AHP analysis will provide a priority order for VPN protocol. In the second (phase 2), the Likert analysis will provide a weighting of competitive advantage elements. And third, text analysis will provide insight into what the users of VPN are thinking while they are using VPN. Using possible relationships factors were organized into the research model shown in Figure 4.5, which contains five constructs at including respondent, research method, result, hypothesis, and security perspective (see figure 4.5). Shared domain knowledge and VPN implementation success are expected to affect both the communication between business and IT and the connections between business and IT strategic planning, which in turn will influence security perspective. In theory, the model in Figure 4.5 should be valid for any organizational unit in which the business and IT have the autonomy to develop their own strategic plans. A limitation of the model is that there is likely to be recursive causality between factors in complex organizations. While acknowledging this limitation, the model was used to guide the research. Also expected was that other relationships and constructs might emerge during the investigation. Several categories of factors were identified that, according to the theoretical and empirical literatures, have the potential to

influence alignment: external influences, IT characteristics, connections between IT and business planning systems, communication between IT and business executives, and implementation of previous IT plans. For the purposes of this research model, to the extent possible, external influences were controlled by collecting data from large organizations and role positions in a large organisation.

4.4.4.2 International Variation

International variation may occur within the data sample between the three international locations. The forecasted response rates will make statistical analysis difficult (a 20% response rate would give 8 items to analyse) and it is anticipated simple summaries of the key determinants in each data type can be compared. This will mean that the international variation analysis will rely on comparisons and be reported as descriptive statements rather than means analysis. The literature reviewed (above) on enterprise size suggests that the international variation should be a minimum and hence descriptive explanation of any observed variation between respective data type should provide adequate power.

A note about obtaining international data, locating international data collecting is usually more difficult in approaching data. Resources, particularly in developing countries, may not be available to collect data as extensively or comprehensively as in the domestic or local. There may also be variations between how data is collected and described between these various agencies. For example, differences in time periods covered, geographic areas, and sample sizes used to tabulate the data will differ. In addition, pay special attention to the definitions and coverage used by each reporting society as the terminology used may have different meanings. Data collecting efforts therefore vary considerably around the world and comparative data may not be available. It is difficult to obtain a precise figure when it comes to national samples. In most cases the numbers reported are estimates. Also, reporting standards and definitions change over time.

4.4.4.3 The Phases 1 – 3

Each of the three data type is collected separately and is to be analysed separately. The forecasted response rate indicates that standard statistical analysis will not be enough to get answers to the research question. As a consequence standardised processing tools will be adopted in the form of the AHP method and the Likert method. Both of these data processing tools are pre-tested and standardised within IS contexts. Although the forecasted response rate is small these tools have proven capability in small response sizes. In the following sections the AHP tool, the Likert tool, and text analysis for unstructured interview data are defined.

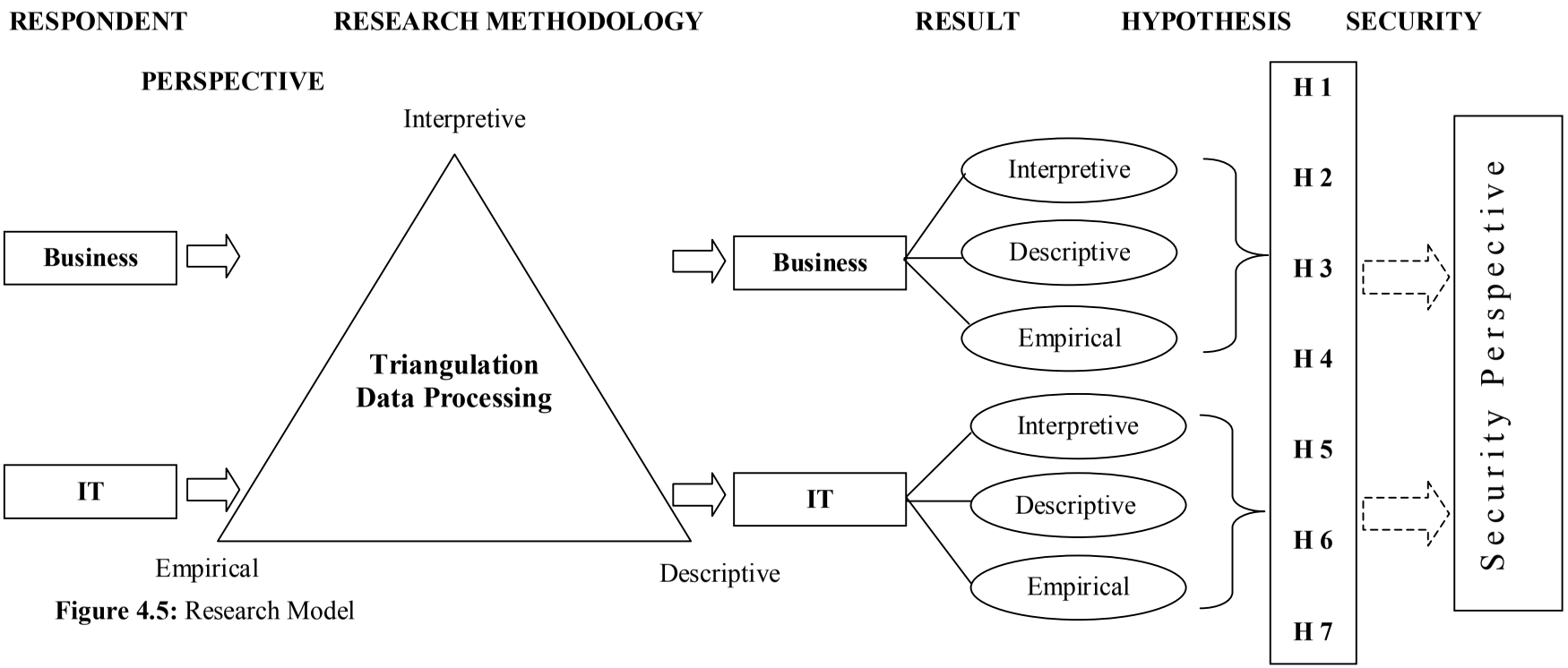

Figure 4.5: Research Model

4.4.4.3.1 AHP expert choice tool

The Analytic Hierarchy Process (AHP) literature has provided a guiding research framework that moves from conceptual level through to measures and explanations. In this instance author adapted the framework to chosen area of study to collect empirical data. The AHP approach has been applied in numerous fields including, previous work for maintenance strategy formulation (Labib, et al., 1997b), intelligent decision analysis (Labib, et al., 1997a), the selection of simulation software (Davis & Williams, 1994), and numerous other applications reported in the work of Zahedi (1986) and Vargas, (1990). Others have also used AHP in a variety of situations such as in supplier selection (Bhutta & Hug, 2002), to determine measures of business performance (Cheng & Li, 2001), and in quantitative construction risk management of a cross-country petroleum pipeline project in India (Dey, 2001).

> AHP methods have been extensively applied and sometimes combined with mathematical programming in developing business and manufacturing system performance evaluation (Lee, et al., 1995; Rangone, 1996), capital rationing (Barbarosoglu & Pinhas, 1995), capital investment decisions (Canada & Sullivan, 1996), advanced manufacturing systems justification and selection (Wabalickis, 1987), and process performance (Frei & Harker, 1999). The analytical hierarchy process (AHP), developed by Saaty (1983), may be applied as a research methodology for the evaluation of information security models. AHP is "a theory of measurement, concerned with deriving dominance priorities from paired comparisons of homogeneous elements with respect to a common criterion or attribute" (Saaty, 1986). AHP imitates the natural tendency of humans to organize decision criteria in a hierarchical form, starting with general criteria and moving to more specific, detailed criteria.

The Analytic Hierarchy Process (AHP) helps the decision maker (business and IT) to prioritize alternatives so that the best one can be selected. The AHP is a mathematically based, multi-objective decision-making tool which was introduced by Saaty (1990). It uses the pair-wise comparison method to rank order alternatives of a problem that are formulated and solved in hierarchical structure. The technique has the advantage of being simple and thorough in handling difficult real-life problems. It provides greater utility in applications where information is either incomplete or not

available. The AHP requires a problem be decomposed into levels, each of which is comprised of elements or factors. The elements of a given level are mutually independent, but comparable to the elements of the same level. The structure presupposes that elements of any given level are influenced by elements at the level immediately above them (see figure 4.4).

In order to assign weights to evaluations areas, factors, and attributes, author used the AHP analysis, which is based on the evaluation framework. Author conducted a questionnaire for business and IT people who have been used VPN as security technology. The weights are evaluated by Expert Choice, which is a multi-attribute decision support software tool based on the AHP methodology and a tool that can help the decision makers to examine and resolve problems involving multiple evaluation criteria. These weights represent a decision maker's judgement on the relative importance or preference of the elements in the hierarchy. The tool for this research is Expert Choice. Expert Choice is a multi-attribute decision support software tool based on the AHP methodology. This tool can help the decision makers (business and IT) to examine and evaluate involving multiple evaluation criteria. The software uses the AHP methodology to model a decision problem and evaluate the desirability of alternatives. The academic and practitioner literature cites several research and application papers involving AHP. The Expert Choice software assists the user in all phases of the problem-solving process, from model formulation to final report output. The structuring module feature assists users in creating an AHP model of the decision problem. The Evaluation and Choice module is the principal component of Expert Choice and is used for creating a model, eliciting expert comparison assessments, solving a model, performing sensitivity analysis, and generating reports. Expert Choice decision models follow the standard AHP format, a functional hierarchy with the broad overall goal or objective at the highest level. Lower levels correspond to the criteria and respective sub-criteria used to choose among alternatives.

For each level, starting at the top of the hierarchy and working down, a number of square matrices are formed from the results of comparing the elements of that level with respect to an element in the upper level (see figure 4.6). A value of 1 shows equal importance and a value higher than 1 shows greater importance of one value over the other. For example, while comparing element A with element B, if A is more important, then a higher number is assigned, whereas if B is more important, the reciprocal of that number is assigned in the comparison matrices. The comparison ratings will be reciprocals of the elements in the lower-left triangle. The largest eigenvalue is then solved and the eigenvector corresponding to the largest eigenvalue (principal eigenvector) is calculated to provide priority for the alternatives.

After forming the comparison matrices, the process moves to the phase of deriving and computing the relative weights for the various elements of each level (with respect to an element in the adjacent upper level), as the components of the normalized eigenvector associated with the largest eigenvalue of the comparison matrix. The composite weights of the decision alternatives are then determined by aggregating the weights through the hierarchy. This is done by following a path from the top of the hierarchy to each alternative at the lowest level and multiplying the weights along each branch and summing the products for each alternative. The result is a set of composite or multi-criteria weights, one for each decision alternative. Based on these composite scores, the alternatives are ranked and the one with the largest weight is selected as the preferred choice. The outcome of the analysis is highly dependent on the hierarchy established by the management and the relative judgments made about the various elements of the problem. The mathematical basis for determining the weights has been established in Saaty (1980).

Author had used analytical hierarchy process (AHP) method, which would help business and IT staff of the organization structure their objectives in a hierarchic framework. Business and IT staff could make judgments about the importance of lower level objectives or alternatives where they have the knowledge of the subject matter. In this model, there were three main alternative Virtual Private Network (VPN) protocols, PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), and IPSec (IP Security), as lower level objectives or alternatives.

In this research methodology, a group decision support system has to derive and synthesize priorities from these judgments. The model is set to determine how well the Virtual Private Network (VPN) as information security device is performing. Additionally, business perspective and technical scenarios can be added to the model, just below the goal; then, business and IT can forecast the likely business perspective and technical scenario as well as the appropriate objectives and measures associated with each scenario.

Three main alternatives VPN tunneling protocols are available today:

- Point-to-Point Tunnelling Protocol (PPTP) is an extension of the remote access Point-to-Point protocol defined in the document by the Internet Engineering Task Force (IETF) titled " the Point-to-Point Protocol for the Transmission of Multi-Protocol Datagram over Point-to-Point Links", referred to as RFC 1171 . Cui & Bassiouni (2003)define PPTP as a network protocol that enables the secure transfer to data from a remote client to a private enterprise server by creating a virtual private network

(VPN) across TCP/IP-based data networks. PPTP supports on-demand, multi-protocol, virtual private networking over public network such as the Internet.

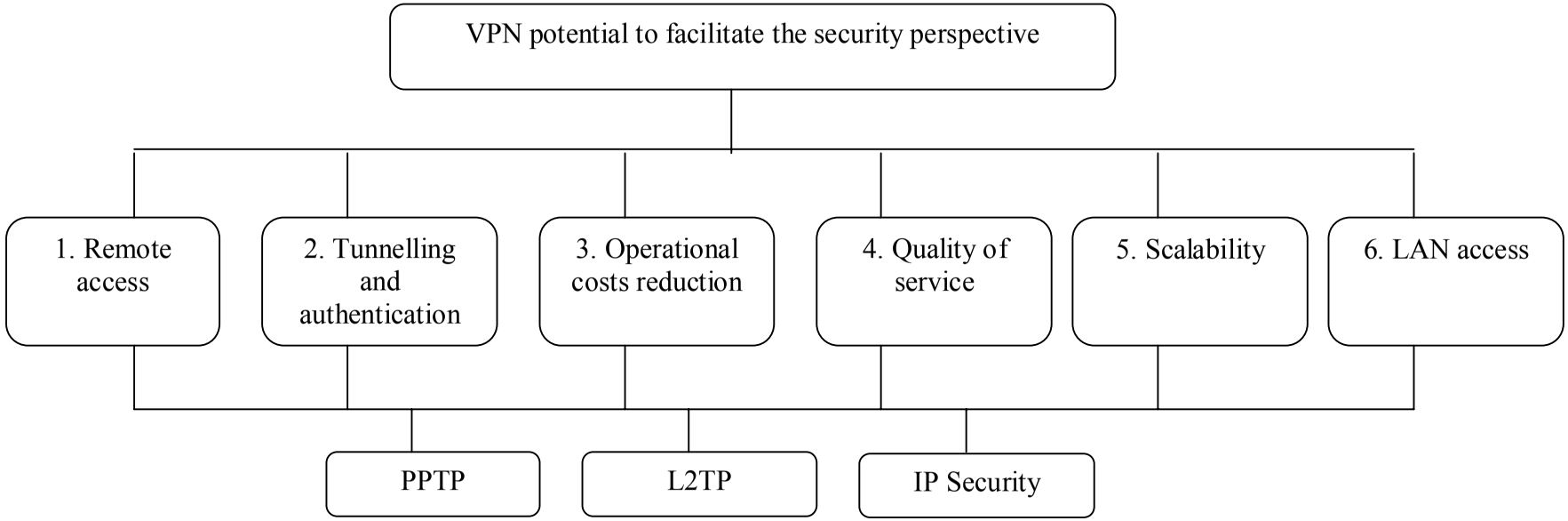

Figure 4.6: VPN performance evaluations

- The Layer 2 Tunnelling Protocol (L2TP) is an emerging Internet Engineering Task Force (IETF) standard that combines the features of two existing tunnelling protocols: Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunnelling (PPTP) (Yuan, Scott, & Erwin, 1998). The Layer 2 Tunnelling Protocol (L2TP), is defined in RFC2661 is a protocol for tunnelling PPP (RFC 1661) sessions over various network types.
- IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provide security for transmission of sensitive information over unprotected networks such as the Internet (Cheung & Misic, 2002). IPsec can be used to protect one or more paths between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

Table 4.3 represents the possible measuring constructs for hierarchical evaluation of determinant attributes of VPN protocol effectiveness.

Table 4.3: AHP Scale

Value	Preference	Explanation
1	Equally important	Two factors contribute equally to the objective
3	Moderately more important	Experience and judgment slightly favor one factor over the other
5	Strongly more important	Experience and judgment strongly favor one factor over another
7	Very strongly more important	A factor is strongly favored and its dominance is demonstrated in practice
9	Extremely more important	Reserved for situations where the difference between the items being compared is so great that they are on the verge of not being directly comparable
2,4,6,8	Intermediate values	To reflect compromise between two adjacent judgments

In this research intended to identify VPN protocol which protocol is most efficient in organization practice. The following main determinant attributes to influence the decision on the best alternative among the existing protocols may be proposed as following:

- Remote access – you are as travelling or home remote user access can gain access to company intranet from a wide range of locations including home.
- Tunnelling and authentication- establishment of data encrypted tunnel between your site and third parties (e.g. distributors, suppliers) and authenticates network user (identifying the user). It must also provide audit and accounting records to show who accessed what information and when.

- Operational costs reduction – VPN makes use of public network resources, business enterprise need not to buy its own networking equipment to cover remote user. Services cost less and deliver high-speed, secure connectivity to every branch location.
- Quality of service – the ability for VPN protocol to obtain the network service it requires for successful operation. VPN offer classes of service and quality of service (QoS) guarantee as the traffic remains within the domain of one network operator and the security afforded by traffic separation is comparable with traditional unencrypted solutions such as frame relay.
- Scalability – A VPN platform should provide an upgrade path for supporting more users, as well as, for integrating new security services, such as virus protection and content filtering.
- LAN access - using a dial-up line to connect a branch office to a corporate LAN. The VPN software uses the connection to the local ISP to create a VPN between the branch office router and the corporate hub router across the Internet.

Table 4.4: Terms and definitions used in the questionnaires

1. Remote access	You are as travelling or home remote user access can gain access to company intranet from a wide range of locations including home.
2. Tunnelling and authentication	Establishment of data encrypted tunnel between your site and third parties (e.g. distributors, suppliers) and authenticates network user (identifying the user).
3. Operational costs reduction	VPN makes use of public network resources, business enterprise need not to buy its own networking equipment to cover remote user. Services costs less and deliver high-speed, secure connectivity to every branch location
4. Quality of service	The ability for VPN protocol to obtain the network service it requires for successful operation. VPN offer classes of service and quality of service (QoS) guarantee as the traffic remains within the domain of one network operator and the security afforded by traffic separation is comparable with traditional unencrypted solutions such as frame relay.
5. Scalability	A VPN platform should provide an upgrade path for supporting more users, as well as, for integrating new security services, such as virus protection and content filtering.
6. LAN access	Using a dial-up line to connect a branch office to a corporate LAN. The VPN software uses the connection to the local ISP to create a VPN between the branch office router and the corporate hub router across the Internet.

4.4.4.3.2 Likert quantification

Survey research is one of the most popular methods used by the information systems researchers (see Section 3 above). Survey research is the systematic gathering of

information from respondents for the purpose of understanding and/or predicting some aspect of the behaviour of the population of interest (Ghanem, 2000). Survey research can be described as a mode of inquiry that involves the collection and organization of systematic data and the statistical analysis of the results (Boudreau, et al., 2001; Wright, Manigault, & Black, 2004). Using a survey research methodology, the researcher can describe large and heterogeneous populations more efficiently and economically. The purpose of quantification is to aggregate through analysis useful information for the answering of the research question (and sub questions).

It is necessary to employ a methodology that permits theoretical propositions to be tested in an objective fashion. The main advantage of survey research is that it gives the researcher a quantitative method for establishing relationships and in this case to understand better the knowledge between business and IT as user perception. In order to test the hypothesized relationships, it is important to use a methodology that would allow the values and relations of constructs to be determined in a systematic way. Survey research is one of the most effective techniques available for the study of attributes, values, beliefs and motives (Bartunek & Seo, 2002; Creswell, 2003; Fowler, 2002). In order to obtain a reasonable sample size to statistically test the research framework and hypotheses, as well as to increase the accuracy of the findings, care is being taken to future proof the field work. This includes allowance for low response rates and pre-tested tools for small samples.

The Likert scale (1932) is a useful analysis tool for use in a full range of sample sizes and psychometric contexts. The small sample sizes can be addressed by reference to (many) similar studies using Likert scales. The respondent indicates agreement, disagreement or shades in between by ticking or clicking an object. The response is an indication of respondent perception and hence there is an attempt to represent a continuum. Similar to the AHP tool imprecise measures are clustered as best fit within pre-determined criteria. This is a different approach to a regression analysis to establish factors and then factor analysis to locate significance (the F-test). Using pre-tested data analysis tools requires the establishment of initial conditions (as discussed and satisfied in Section 3 above) and then the correct use of the tool in the data collection field. The analysis in this case can proceed with descriptive statistics including frequencies, means, medians, and standard deviations. Descriptive statistics are used to describe the basic features of the data and to test hypothesis in this study. A one Sample T Test is used to determine whether or not the mean Likert response scale 1 – 5 of the question in each sample significantly differ from 1 through 5 of the likert response scale (1= strongly disagree, 2 = disagree, 3 = undecided, 4 = agree, and 5 = strongly agree). The one-sample t test can be used whenever sample means must be compared to a known test value.

Hence the survey responses are to be collected in a data base and then imported into SPSS for analysis.

The exploratory studies consist of descriptive statistics. The exploratory study begins with a descriptive statistics analysis to examine: (1) normality of the score distribution for each item and (2) how important the respondents rated each item (see tables). Descriptive Statistics are used to present quantitative descriptions in a manageable form. They provide simple summaries about the sample and the measures. Descriptive statistics simply describe what was or what the data represents. Descriptive statistics are hence were used to describe the basic features of the data in this study. SPSS statistical procedures were used to analyse the data. Once all the responses were gathered, the output was transferred again from the Access database to SPSS where all analysis and calculations were performed. SPSS statistical software package allows the researcher to conduct the rigorous analyses needed to answer the research question and sub-research questions which this study asked to investigate. The values assigned to the answers for the positive 1-5 Likert response scale items were flipped so that "strongly agree" would have a value of 5 and "strongly disagree" would have a value of 1 for negatively worded items. The competitive advantage data was imported into SPSS for analysis. They provided simple summaries about the sample and the measures. Together with simple graphics analysis, they form the basis of virtually every quantitative analysis of data.

In this phase, the central tendency of a distribution is an estimate of the centre of a distribution of values including mean, median, and standard deviation. The Mean or average is probably the most commonly used method of describing central tendency. The Median is the score found at the exact middle of the set of values. The Standard Deviation is a more accurate and detailed estimate of dispersion because an outlier can greatly exaggerate the range. The Standard Deviation shows the relation that set of scores has to the mean of the sample. The frequencies procedure provides statistics that are useful for describing variables that cluster (in for example, Likert scales). The Frequencies procedure is useful for obtaining summaries of individual variables. 3D Scatter provide visualisation of the relationship between quantitative questionnaires as variables by plotting the actual values along three axes. They often present relationships, such as a curvilinear pattern, that descriptive statistics do not reveal, and they can uncover bivariate outliers.

The Likert tool is described as:

> "Likert scaling is a bipolar scaling method measuring either positive or negative response to a statement. Sometimes Likert scales are used in a forced choice method where the middle option of "Neither agree nor disagree" is not available. Likert scales may be subject to distortion from several causes. Respondents may

avoid using extreme catagories (central tendancy bias); agree with statements as presented (acquiescence response bias); or try to portray themselves or their group in a more favorable light (social desirability bias). After the questionnaire is completed, each item may be analyzed separately or item responses may be summed to create a score for a group of items. Hence, Likert scales are often called summative scales. Responses to a single Likert item are normally treated as ordinal data, because, especially when using only five levels, one cannot assume that respondents perceive the difference between adjacent levels as equidistant. When treated as ordinal data, Likert responses can be analyzed using non-parametric tests, such as the Mann-Whitney test, the Wilcoxon signed-rank test, and the Kruskal-Wallis test. When responses to several Likert items are summed, they may be treated as interval data measuring a latent variable. If the summed responses are normally distributed, parametric statistical tests such as the analysis of variance can be applied. Data from Likert scales are sometimes reduced to the nominal level by combining all agree and disagree responses into two categories of "accept" and "reject". The Cochran Q, or McNemar-Test are common statistical procedures used after this transformation. Consensus based assessment (CBA) can be used to create an objective standard for Likert scales in domains where no generally accepted standard or objective standard exists. Consensus based assessment (CBA) can be used to refine or even validate generally accepted standards." (Direct Quote: http://en.wikipedia.org/wiki/Likert_scale)

4.4.4.3.3 Unstructured interview

An unstructured interview is undertaken to let the user talk about what they are doing and to respond to lead questions. In addition the user can be observed both in terms of their actions on the computer screen and personal body language (see Section 6.2.3). This is interpretative data because the interviewer is influencing the user and providing guided stimulus for their responses. There are also feedback loops where the interviewer may paraphrase responses to elicit further elaboration, or the interviewer may ask for clarification of any statement or event in the study space. The data consequently can be collected using a variety of techniques. For example, a video and audio recording, check sheets, and any other appropriate recording modes. The analysis of this data can then proceed by using a variety of techniques. For example, exception analysis, frame analysis, profile selection, text analysis, clustering, descriptive summary, and so on. Appropriate tools for this are SPSS, NVIVO, and hand mapping. Qualitative research methods are designed to help researchers understand people and the social and cultural contexts within which they live. The data analysis is therefore less structured and more

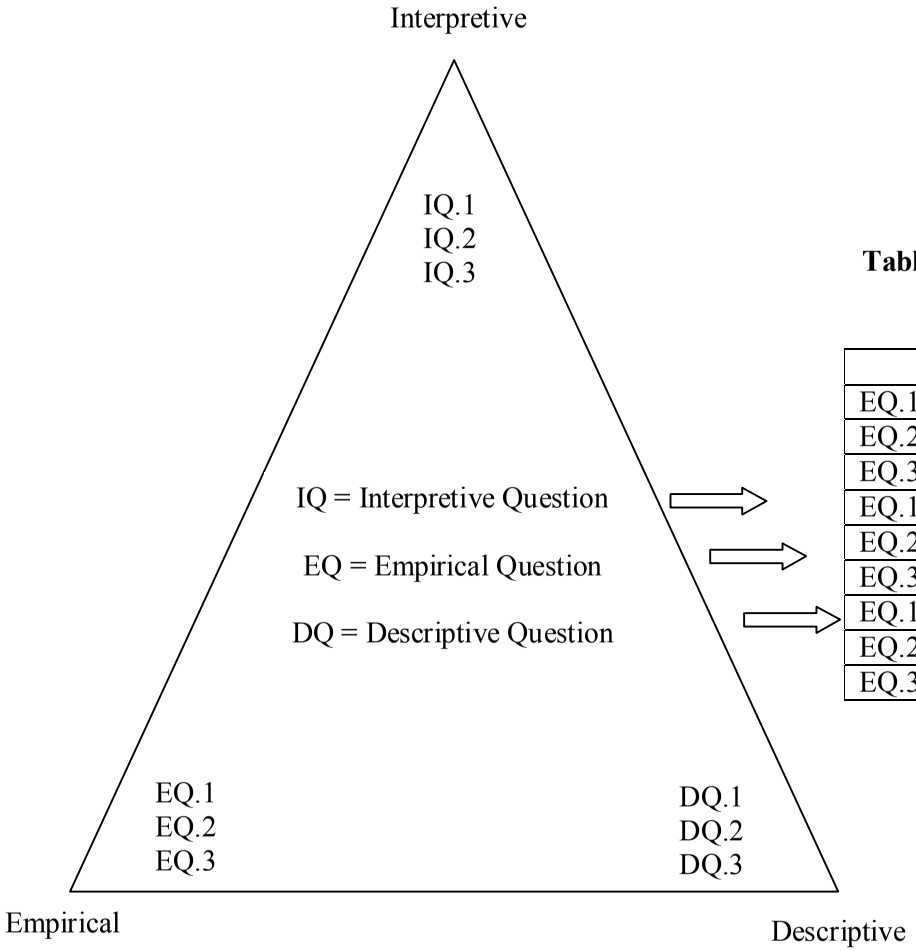

Table 4.4: Triangulation Clusters

Triangulation Clusters		
EQ.1 &. IQ.1	DQ.1 & IQ.1	EQ.1 & DQ.1
EQ.2 & IQ.1	DQ.2 & IQ.1	EQ.2 & DQ.1
EQ.3 & IQ.1	DQ.3 & IQ.1	EQ.3 & DQ.1
EQ.1 & IQ.2	DQ.1 & IQ.2	EQ.1 & DQ.2
EQ.2 & IQ.2	DQ.2 & IQ.2	EQ.2 & DQ.2
EQ.3 & IQ.2	DQ.3 & IQ.2	EQ.3 & DQ.2
EQ.1 & IQ.3	DQ.1 &. IQ.3	EQ.1 &DQ.3
EQ.2 & IQ.3	DQ.2 & IQ.3	EQ.2 & DQ.3
EQ.3 & IQ.3	DQ.3 & IQ.3	EQ.3 & DQ.3

Figure 4.7: Triangulation Design and Data Collection

interpretive than for example questionnaire data analysis. The way people express themselves is context bound and the interpretation can be anchored to the contextual factors. However, in an unstructured situation elements may overlap, the object of discussion be obscured by other competing emotions & agendas, and the world of the user conflict with the research framework. Good analysis is able to separate obscurities and to connect meaningful relationships.

4.4.4.3.4 Triangulation

Triangulation (as discussed in Section 4.2.4) is used in terms of the different data types in this study. Empirical, descriptive and interpretative data types were chosen to respond to some of the problems identified by others doing IS research (see Sections 4.2.0 and 4.3). The data analysis was structured to identify relationships within each independent group of data type but the review of prior research suggests that significant relationships can also be found between the data types. Hence the data types are to be triangulated by taking each data type in combination with every other data type. Table 4.1 defines each of the possible relationships that may give rise to additional findings. All redundancies are removed to leave only possible additional relationships. The logical relations are coded EQ (empirical), DQ (descriptive), and IQ (interpretative). A redundancy for triangulation would be the permutation EEEQ as this has been treated in Phase 1, and so on. Similarly EEIQ is the same as EIEQ and may be reduced to the pair EIQ which is the same as IEQ. Hence the number of possible logical relationships reduces from 27 (3^3) to 18, and are defined in Table 4.4. The data treatment technique will be to look for exceptions in the phases 1 – 3 data analysis and to retain the exceptions as additional findings in the study (see Figure 4.7).

4.4.5 Hypothesis Testing and Truth Claims

The statistical testing of hypotheses is a process whereby the researcher decides if a result is significant in terms of the evidence collected within any given experimental design. The decision for the researcher is to accept the result as being exceptional and related to the intervention, or to reject the result as being easily explained by chance. The logic is based on inference and the result is accepted to be causal (rather than only correlated). One further element is also required to decide the merit of any given result. That is a comparative set of data that has been produced by others doing similar studies.

> "To make this decision (the researcher) must in some way produce a relevant reference set that represents a characteristic set of outcomes which could occur if the modification was entirely without effect. The actual outcome may then be compared

with this reference set. If it is found to be exceptional, the result is declared statistically significant." (Box, et al., 1978, p. 22).

The outcome of the hypothesis testing procedure is to establish that an intervention has a significant effect or that it does not. A further step once the effect has been identified as significant is to then develop estimates (confidence intervals) for the size of the effect. All of these steps, procedures and processes are standard statistical ways of testing hypothesis.

The approach in the current study is the hybrid approach (see Section 2.4 above). In a hybrid approach the standard statistical methods are useful guidelines as to how to proceed in testing hypothesis, but statistical method does not provide a complete explanation for all decisions that are made in a hybrid context. For example, quantified interpretative data may not match closely with the VPN or the immediate context (ie. uncontrolled variables and / or interaction of variables are contributing to the effect) and a standard hypothesis test would likely produce an erroneous result. In a context (experimental design) where greater controls may be asserted over the design inputs this would not be a problem. The hybrid approach was designed to mitigate the interaction of variables in complex and dynamic IS contexts. For example the evidence resident in human mental maps may not be accessible through questionnaires but interviewing can give access. The use of many data collection techniques and data types required a different mapping of data to testing. The principal method for reliability measure and inclusion of data in a study was the use of triangulation at both / either - or the data level or at the case level (see Section 6.4.3). Triangulation hence provides a measure of trust others may put in findings. Data becomes networked and connect to other data in ways that singular results are valid only in relation to the network outcomes. The statistical hypothesis testing process is shifted from the main emphasis being placed on the outcome of a test and towards the network of data that provided evidence for the claims. In effect statistical method has this feedback loop built into the process because any outcome requires further comparison against benchmark data and common sense appraisal against the substantive context. However, in a hybrid approach, hypothesis testing is more complex and account must be given of the inter-relatedness of data. A hypothesis may be tested by correlating the accumulated evidence for a hypothesis, neutral material, and evidence against a hypothesis. The adjudication of the result is hence based on a reasoned argument that considers the competing weighting of evidence and may be expressed as a series of trade-offs.

Consequently, truth claims in a hybrid research context are substantiated by the construct of evidence and mitigated by declared limits to the network. Results may be

qualified and not just accepted or rejected. The justification and explanation of claims is evidential and the limits of transfer are expressed in terms of the relative value of evidence within the supporting evidence. For example a statement that asserted hypothesis H49 is accepted must be qualified by statements defining the grounds on which it was accepted and the logical reasons for the preference of acceptance data over rejection data. The hybrid research approach is hence reliant on explanation and elaboration to a greater extent than the statistical interpretation of hypothesis testing and subsequent claims of truth. It may be argued that the difference is in expression rather than at the substantiative level as both approaches require rigorous adherence to procedure. In this research the hypotheses are to be tested by first systematically compiling all evidence for, against, and neutral to each of the nine hypothesis. The evidence is to be collected in tables at the end of each phase and the triangulation. The evidence can then be weighted by counting the number of evidence statements in each column, and then by weighting the value of each statement (on a scale 1 – 5 (low to high)) for the relative worth of the evidence in the network, and by the actual worth (on a scale 1 – 5 (low to high)) with respect to the data type and the triangulation. Hence a total score for each column may be calculated by adapting the standard weight function ($T_i = \sum w_i x_i$). Hence the total for a column would be arrived at by adding the relative and actual values into a total sum. A final result may be gained by taking the highest total of the columns, or if the totals are close by subtracting the 'for' from the 'against' (and vice versa), or by pairing the two winning numbers. In this way a hypothesis may be accepted or rejected or nullified.

4.5 CONCLUSION

In this chapter a methodology was developed that would best answer the research question. A hybrid research approach was chosen to mitigate forecasted deficits in the proposed research field. The deficits were identified from other related IS studies where the response rates were low, the variance was wide in medium and small businesses, and the data range has been claimed to be too narrow in answering IS questions. The theoretical exploration of research approaches concluded that there are many ways of approaching studies in IS and that none has absolute priority over another. As a consequence a researcher has considerable space to move in and to develop appropriate methods and procedures that best suit the context and the research question.

The research design adopted triangulation at the data and case levels so that reliability could be assured and validity asserted. The problem area for research was

conceptualised to be a three dimensional interspace between work systems, the security technology, and the business performance requirements. As a consequence the target data for collection had several characteristics. Three different data collection methods were adopted and tools developed to collect and process the different data types. A strong attempt was made to select a sample that minimised bias and that provided conditioning of input variables that would be best filtered from the study. As a consequence a triangulated international sample was selected in large companies. The ideal sample was for 120 respondents in three different international jurisdictions and divided into 20 IT and 20 business respondents in each location. The risks of bias and of transfer are managed within the design. However, the limits of the approach are acknowledged. The extent the findings may be transferred to other contexts or the findings replicated in other research are less than the explanatory power that may be gained by knowing the wider picture of IS implementation.

This Chapter provides the link between the literature review and the field work. It is necessarily a discussion of theoretical design and pragmatic expectations, and a definition of WHAT ideally is to occur in the field. Many of the objects of study are not tangible and hence a variety of strategies have been spelled out to collect the necessary information that the research question, its sub-questions, and hypothesis may be adequately addressed. The potential contribution is for MIS practitioners, especially for information security whose business models and revenue streams are based on long-term usage of IT products and services. Effective management of long-term usage requires ex ante identification of belief and attitude changes (that govern long-term usage) and understanding the key levers of such changes. Such understanding can assist in the proactive planning of intervention mechanisms (e.g., user training) for minimizing the probability and impacts of change. Hence the the important outcomes of the research will include the theory development for setting objectives that can assure effectiveness of computer network security systems, as well as policy parameters for managerial implementation of secure network systems. Protected action can then be explained in terms of each possible permutation within the VPN, Work systems, and Competitive Advantage context, and justified within the proposed network of truth claims.

CHAPTER 5

RESEARCH FINDINGS

5.0 INTRODUCTION

The data collection proceeded according to the specifications defined in Chapter 4. This chapter reports the variations to the research plan and the analysis of data. The research in Chapter 4 proved adequate in scope to allow the researcher to collect sufficient data that the research question may be answered. The difficulties reported by other researchers collecting data in the IS context were apparent. Initially it was difficult to get co-operation for the pilot study, and then access to enterprise systems was even more difficult. The strategy of triangulating the study across three different international jurisdictions gave a greater number of large enterprises to approach. One in each of the jurisdictions was eventually gained. Once this had been established the response rate issue came to the fore. All of these problems and characteristics of the IS research field had been foreshadowed by others.

This chapter is organised to first report and discuss the problems and response rates gained in the study, and to report the analysis of international variations. Section 2 is then divided into the three independent phases of analysis. These phases corresponded to the different data type that were collected and the unique three sub-questions that related to each data type. Each subsection is structured to first report the overall findings, the business – IT strata analysis, and in conclusion a summary of evidence (a table) that links the findings to the sub questions. Section 3 demonstrated the highest level of analysis where the independent findings of phases 1 – 3 are triangulated to identify exceptions and to collect any further evidence that may be used to test the nine hypotheses. The testing of hypotheses proceeds according to the specification in Section 4.6.5 and is reported in tables of evidence that are adjudicated by the decision metric (see Section 4.6.5).

5.1 FIELD FINDINGS

The field findings came from three events, namely: the pilot study, the problems encountered and the field intervention. These findings had the characteristics determined in Chapter 4, namely: questionnaire feedback, response rates, the actual cases gained, and the international variations. In addition the data was collected from the intervention and made available for processing. Consequently the field findings are reported under these headings.

5.1.1 Pilot Study

The pilot study was conducted with three IT professionals and three business excutives. The purpose was to validate the survey and questionnire and to gain feedback on both communication and conceptual levels. The IT professionals and business executives were chosen because they had experience in information security and used VPN for their business processing and transactions. Feedback could help to improve communication and correct any contradictions in the surveys. Also feedback on the survey's length, its overall appearance, and participants' comfort with the instruments could be gained. Comments and suggestions feedback were hence used to revise the survey.

In the pilot study, author met with each of the participants individually and briefly reviewed the purpose of the survey. Initially all of the participants said they would do the pilot but four never returned the feedback forms. This left six completed returns. When followed up two could not be contacted and the other two cited work pressures and regretfully a lack of time. All participants were asked to read the cover letter and complete the survey. They were also asked for suggestions to identify VPN features, VPN user observation, competitive advantage attributes, and unclear meanings in the survey. These could improve on the three surveys that had been used for data collecting by others and modified by the researcher. The feedback suggested that some of questions on AHP and VPN features required changing to beter focus on enduser attributes and to reduced the length. IT professionals in particular requested the deletion of 11 questions and the insertion of four. The comments of each participant were used to revise the survey before a final meeting. In addition to substantially improving the clarity of the survey definitions and items, the comments permitted a reduction in the number of business items as following competitative advantage reduced from 19 to 17, VPN observation question reduced from 10 to 7. These responses were then compiled and change made to the web site and questionnaire presentation to better forecast respondent’s expectations.

The revised questionnaires were uploaded on a web server and four pilot members were asked to give feedback on the online questionnaire. An additional goal of the piloting process specific to online surveys was to have participants submit the survey from a variety of computers and Internet connections, using different browsers (Netscape, Internet Explorer), including all possible versions, on different platforms (Macintosh and Windows). This was also to test if respondents would complete the survey, click on the submit button, and that researcher should receive the survey by email. The e-mail survey involved a computerized, self-administered questionnaire, which the researcher sent and the respondents

received, completed, and returned through e-mail systems. In this piloting process, the researcher received completed web-based surveys from all the respondents by email.

Through online survey piloting, researcher had encountered unanticipated consequences that either delayed or aborted feedback. Respondents reported that the online surveys were too long. As a result, the researcher modularized the questionnaires offering only one module to subjects with the option of completing additional modules at the end of the survey. Web specific question structuring problems had been revealed through piloting. These problems included but were not limited to such items as: too many open-ended questions, incorrect defaults (hidden or revealed), large enough text boxes that scroll, question independence (so one mistake did not invalidate the complete survey), ambiguous wording, inconsistent terminology, non-orthogonal categories, overlapping categories, and answers that cannot be undone.

One IT professional suggested that the technique of displaying each question separately a screen would give participants choice where they are not forced to provide an answer before moving on. Also each page of the questionnaire could be downloaded separately from the server and not allowed to reside in the Web browser's cache memory. This makes for an awkward and time-consuming survey taking process. In one pilot case, subjects consistently abandoned the survey at the same point allowing the researcher to identify unclear instructions as the reason for survey abandonment.

5.1.2 Problems Encountered

The first problem the researcher encountered was access to respondents and then once access was gained that many who said they would do the surveys did not return copy in any form. Initially contacts were identified from lists of large companies in big cities in New Jersey, Bangkok and Auckland. These locations were chosen because large companies were in these locations and also the researcher had worked in each of these regions and had professional contacts. The university list of business contacts was also used for making initial contact. Author found out some problem of online questionnaire of response types that include: complete responders, unit responders (did not participate at all), answering drop-outs, viewed but did not answer questions, viewed some but not all of the survey, item non-responders (only answered some of the questions, but completed the survey), and item non-responding drop-outs (answered some questions, but dropped out before completing).

Author found that data collecting both business and IT in Auckland, New Zealand was insufficient to support research question and sub-questions including testing hypothesis.

Faced with the problem of data collecting in Auckland, New Zealand entities seem to be limited information security resource and more conservative in their view of information technology (IT) resources. Author needed to collect data from other 2 countries including Bangkok, Thailand and New Jersey, USA. In this way, Author could combine qualitative and quantitative methods to test the validity of results (triangulation), to improve data collection instruments, and to explain findings as more research value.

5.1.3 Response Rates

In phase one the data response rate came from survey questionnaires online on VPN perception of security users. The researcher set up VPN perception of user (see appendix) and 120 VPN perception of user questionnaire online were sent to business (60) and IT (60). There were 45 of respondents or about 37% of 120 questionnaires, 24 (40%) for business respondents and 21 (35%) for IT respondents.

In phase two of data responding, author used survey questionnaires online on competitive advantage on VPN. Author sent 120 competitive advantage questionnaires to business (60) and IT (60) via Internet. There were 48 of respondents or about 40% of 120 questionnaires, 26 (43%) for business respondents and 22 (36%) for IT respondents.

Finally, author used observation and unstructured interview methods on VPN users by visiting VPN users at their work places. There were 25 VPN users whom author had observed at work place. Author used data sheet (see appendix) to collect and observed VPN users. Each user had been observed by author for 15 – 20 minutes. The researcher complied with the specification defined in Chapter 4.

5.1.4 The Field Cases

Three enterprise systems were responsive to the researcher. The first was in Auckland and from the insurance industry. It was a large company (as per Chapter 4 definition) with 250+ staff and an annual turnover greater than us$2 billion. It was structured into vertical silos with different divisions of corporate functionality being distributed in different managerial portfolios. The IT manager was the contact point. She chose a 50:50 split between business and IT VPN users. The choice of participant was made on the frequency of use and years of experience. Each participant had the option to opt out if they wished. The non-response rate was high with only 6 completed responses out of the 40 chosen and agreed to respondents. The reasons for non-response were given as time constraint, disclosure concerns and competing agendas in the work space.

The second enterprise system was in Bangkok and from the communications industry. It was a large company with 300+ staff and an annual turnover of greater than us$8 billion. As this was a large company it was structured similar to the Auckland and New Jersey enterprise systems. It was structured into vertical silos with different divisions of corporate functionality being distributed in different managerial portfolios. The general manager was the point of contact. He chose a 50:50 split between business and IT VPN users. The choice of participant was made on the frequency of use and years of experience. Each participant had the option to opt out if they wished. The non-response rate was lower than Auckland with 12 completed responses out of the 40 chosen and agreed to respondents. The reasons for non-response were the same as Auckland. These were given as time constraint, disclosure concerns and competing agendas in the work space.

The final large enterprise system was in Jersey City New Jersey and from the IT software industry. It was a large company with 400+ staff and an annual turnover of greater than us$15 billion. As this was a large company it was structured similar to the Auckland and Bangkok enterprise systems. It was structured into vertical silos with different divisions of corporate functionality being distributed in different managerial portfolios. The sales manager was the point of contact. He chose a 50:50 split between business and IT VPN users. The choice of participant was made on the frequency of use and years of experience. Each participant had the option to opt out if they wished. The non-response rate was higher than Bangkok- with 8 completed responses out of the 40 chosen and agreed to respondents. The reasons for non-response were the similar to Auckland and Bangkok, but also included statements to the effect that the question range was too wide (ie. business and IT) and outran the respondent knowledge range.

5.1.5 International Variations

In table 5.1 and 5.2 represent data of each country which had collected as triangulation and international data collection. Researcher had sent online questionnaire to 40 respondents (20 businesses and 20 ITs) in each country and asked each respondent to visit the web page to complete the online questionnaire. In table 5.1 phase one, the total of respondents is 45 which splits in between business and IT in each country (see table 5.1). Table 5.2 phase two, the total of respondents is 48 and the number of each business and IT show in columns where the first column show each country (see table 5.2).

Table 5.1 Phase one triangulation and international data collection

Triangulation and International Data Collection Phase One					
Country	Online Propose	Business	IT	Total	Percentage
New Zealand	40	8	7	15	34%
Thailand	40	9	8	17	33%
USA	40	7	6	13	33%
Total	120	24	21	45	100%

Table 5.2 Phase two triangulation and international data collection

Triangulation and International Data Collection Phase Two					
Country	Online Propose	Business	IT	Total	Percentage
New Zealand	40	9	8	17	34%
Thailand	40	9	7	16	33%
USA	40	8	7	15	33%
Total	120	26	22	48	100%

In table 5.3 shows observation data collection as triangulation where first column represents each country. Research used observation method on VPN user attitude by visiting VPN users at their work places and giving observation question sheet to business and IT. The total of VPN user is 25 and represents in the total column which can distinguish in business and IT columns (see table 5.3).

Table 5.3 Phase three triangulation and international observation

Triangulation and International Data Collection Phase Three					
Country	Online Propose	Business	IT	Total	Percentage
New Zealand	40	4	3	7	31%
Thailand	40	6	6	12	46%
USA	40	3	3	6	23%
Total	120	13	12	25	100%

5.1.6 Phase One of Data Analysis

In this phase, the used analytical hierarchy process (AHP) method, which would help business and IT staff of the organization structure their objectives in a hierarchic framework. Answers to the research sub-questions in section 3 of chapter 4 as following: (i) what measures are critical for MIS security? , (ii) what is the relationship between IT and Business objectives for optimal security assurance?, and What elements are required in the MIS to assure protection?

- What measures are critical for MIS security?
- What is the relationship between Business and IT objectives for optimal security assurance?
- What elements are required in the MIS to assure protection?

The Analytic Hierarchy Process (AHP) is a methodology for structuring, measurement, and synthesis. The AHP has been applied to a wide range of problem situations selecting among competing alternatives in a multi-objective environment, the allocation of scarce resources, and forecasting. Although it has wide applicability, the axiomatic foundation of the AHP carefully delimits the scope of the problem environment. It is based on the well defined mathematical structure of consistent matrices and their associated right-eigenvector's ability to generate true or approximate weights.

Any hierarchical-based methodology must use ratio-scale priorities for elements above the lowest level of the hierarchy. This is necessary because the priorities (or weights) of the elements at any level of the hierarchy are determined by multiplying the priorities of the elements in that level by the priorities of the parent element. Because the product of two interval-level measures is mathematically meaningless, ratio scales are required for this multiplication. Since, the AHP utilizes ratio scales for even the lowest level of the hierarchy (the alternatives in a choice model), the resulting priorities for alternatives in an AHP model will be ratio-scale measures. This is particularly important if the priorities are to be used not only in choice applications, but for other types of applications such as forecasting and resource allocation. Choice decisions involve the selection of one alternative from a given set of alternatives, usually in a multi-criteria environment. Typical situations include product selection, vendor selection, structure of an organization, and policy decisions.

5.1.6.1 Research findings

In phase one research findings, the model should structure the analysis process for decision-making, including important aspects, such as criteria grouping (respecting the independence between them), clarity, predictability and completion of the set of criteria. In addition, the implementation of the computational model would allow for the criteria voting to be done in an organized way, taking the inherent logic sequence of a decision into consideration. In this model, there were three main alternative Virtual Private Network (VPN) protocols, PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), and IPSec (IP Security), as lower level objectives or alternatives. There were 6 main determinant attributes of VPN protocol features to influence the decision on the best alternative among the existing protocols may be proposed as following remote access, tunnelling and authentication, operational costs reduction, quality of service, scalability, and LAN access. Business and IT staff could make judgments about the importance of lower level objectives or alternatives where they have the knowledge of the subject matter.

In table 5.4 shows over all of AHP ratio-scale measures on evaluated VPN protocols as empirical in this phase, which contains details constructs in columns including respondents, determinant attributes of VPN protocol and three main alternative Virtual Private Network (VPN) protocols (IP security, L2TP, and PPTP).

Table 5.4 AHP ratio-scale

45 Respondents	
VPN protocol priorities with respect to "***Remote access***"	
Business	
IP Security	0.526
L2TP	0.326
PPTP	0.197
IT	
IP Security	0.498
L2TP	0.316
PPTP	0.185
VPN protocol priorities with respect to "***Tunnelling and authentication***"	
Business	
IP Security	0.575
L2TP	0.348
PPTP	0.196
IT	
IP Security	0.518
L2TP	0.322
PPTP	0.204
VPN protocol priorities with respect to "***Operational costs***	

reduction"	
Business	
IP Security	0.593
L2TP	0.312
PPTP	0.180
IT	
IP Security	0.449
L2TP	0.324
PPTP	0.223
VPN protocol priorities with respect to "***Quality of service***"	
Business	
IP Security	0.499
L2TP	0.316
PPTP	0.187
IT	
IP Security	0.598
L2TP	0.557
PPTP	0.309
VPN protocol priorities with respect to "***Scalability***"	
Business	
IP Security	0.452
L2TP	0.327
PPTP	0.219
IT	
IP Security	0.583
L2TP	0.542
PPTP	0.300
VPN protocol priorities with respect to "***LAN access*** "	
Business	
IP Security	0.408
L2TP	0.293
PPTP	0.182
IT	
IP Security	0.406
L2TP	0.291
PPTP	0.187

5.1.6.2 Business and IT Finding

In this result, both business and IT people had weighted VPN protocols with respect to each information security features (see table 5.5). In table 5.5, while comparing VPN protocols with respect to “Operational costs reduction” (see table 5.5) business people weighted more importance on IP Security at 0.593 than other two VPN protocols (L2TP and PPTP). Second, business people had weighted, as the preferred choice, on IP Security at 0.575 with respect to “Tunnelling and authentication” following by L2TP at 0.348 and PPTP at 0.196. IP Security at 0.526 came in third priority with the respect of “Remote access” which had weighted by

business people. While comparing VPN protocols with other respects ("Quality of Service", "Scalability", and "LAN access") business people weighted more importance on IP Security.

According to table 5.5, IT people had weighted the importance of VPN protocols (IP Security, L2TP, and PPTP) in different respective of information security features. For example, IT people made decision or weighted on IP Security at 0.598 and as the first priority with respective of "Quality of Service". Author noticed business people selected or chose IP Security as the first priority but different respective which was "Operational costs reduction" (as above). Furthermore, IT people weighted the important of IP Security at 0.583 with respect to "Scalability" as second priority. Business people weighted more importance of IP Security at .0575 with respect to "Tunnelling and authentication". IT and business people had weighted IP Security as the same result but there were different with respects of information security features as different priority orders. Inconsistent expert judgment can be a factor when using the pairwise comparison method. The Evaluation and Choice module calculates and displays the inconsistency ratio (IR) of the AHP technique. The IR of 0.07 was obtained in this example. The IR provides a measure of the logical rationality of the pairwise comparisons: a value less than 0.10 is generally considered acceptable.

Table 5.5 comparing of the importance of VPN protocol with respective of features

	24 Business Respondents	**21 IT Respondents**
VPN protocol priorities with respect to "***Remote access***"		
IP Security	0.526 (Strongly more important)	0.498 (Intermediate Value)
L2TP	0.326 (Moderately more important)	0.316 (Moderately more important)
PPTP	0.197 (Equally important)	0.185 (Equally important)
VPN protocol priorities with respect to "***Tunnelling and authentication***"		
IP Security	0.575 (Strongly more important)	0.518 (Strongly more important)
L2TP	0.348 (Moderately more important)	0.322 (Moderately more important)
PPTP	0.196 (Equally important)	0.204 (Intermediate Value)
VPN protocol priorities with respect to "***Operational costs reduction***"		
IP Security	0.593 (Strongly more important)	0.449 (Intermediate Value)
L2TP	0.312 (Moderately more important)	0.324 (Moderately more important)
PPTP	0.180 (Equally important)	0.223 (Intermediate Value)
VPN protocol priorities with respect to "***Quality of service***"		
IP Security	0.499 (Intermediate Value)	0.598 (Strongly more important)
L2TP	0.316 (Moderately more important)	0.557 (Strongly more important)
PPTP	0.187 (Equally important)	0.309 (Moderately more important)
VPN protocol priorities with respect to "***Scalability***"		
IP Security	0.452 (Intermediate Value)	0.583 (Strongly more important)
	0.327 (Moderately more important)	0.542 (Strongly more important)

L2TP		
PPTP	0.219 (Intermediate Value)	0.300 (Moderately more important)
VPN protocol priorities with respect to "***LAN access*** "		
IP Security	0.408 (Intermediate Value)	0.406 (Intermediate Value)
L2TP	0.293 (Intermediate Value)	0.291 (Intermediate Value)
PPTP	0.182 (Equally important)	0.187 (Equally important)

In these results analytical hierarchy process (AHP) method, this would distinguish the different perspective between business executive and IT professional of the organization structures their objectives in a hierarchic framework. Based on these composite scores, the alternatives are ranked and the one with the largest weight is selected as the preferred choice (see tables 5.6). Their judgments are based on the importance of lower level objectives or alternatives where they have the knowledge of the subject matter. These results of AHP ratio-scale between Business and IT could notify the significant difference between business and IT objective (hypotheses 1). AHP ratio-scale could illustrate business objective bias can significantly predict systems capability (hypotheses 5) such as VPN security technology. The outcome of the analysis could advise IT objective can significantly improved business performance (hypotheses 4) by using VPN system in their organizations.

In table 5.6 shows comparing of the importance of information security features between business and IT. In table 5.6, business people weighted more importance on "Operational costs reduction" as first priority at 0.598 and "LAN access" was last priority at 0.434 (see table 5.6). On other hand, IT people weighted importance on "Quality of Service" as first priority at 0.603 and "LAN access" was last priority at 0.414 (see table 5.6).

Table 5.6 comparing of the importance of information security features

	24 Business Respondents	**21 IT Respondents**
Remote access	**0.537**	**0.507**
Tunnelling and Authentication	**0.584**	**0.547**
Operational costs reduction	**0.598**	**0.452**
Quality of service	**0.502**	**0.603**
Scalability	**0.459**	**0.585**

LAN access	**0.434**	**0.414**

Results are grouped by the construct being measured and tabulate by method of data collection. In tables 5.4 and 5.5 show empirical result between business and IT. First column shows priority in ascending order; second column shows VPN protocol; third column shows weight by AHP scale; last column shows for example business people weighted importance on IP Security at 0.593 with respect to Operational cost reduction was at the first priority. On other hand, IT people weighted IP Security at 0.449 with respect to Operational cost reduction in different priority order which was rank number 5.

Table 5.7 Empirical AHP Result by Business

Ascending Priority	VPN Protocol	Weight	Respective
1	IP Security	0.593	Operational costs reduction
	L2TP	0.312	
	PPTP	0.180	
2	IP Security	0.575	Tunnelling and authentication
	L2TP	0.348	
	PPTP	0.196	
3	IP Security	0.526	Remote Access
	L2TP	0.326	
	PPTP	0.197	
4	IP Security	0.499	Quality of Service
	L2TP	0.316	
	PPTP	0.187	
5	IP Security	0.452	Scalability
	L2TP	0.327	
	PPTP	0.219	
6	IP Security	0.408	LAN Access
	L2TP	0.293	
	PPTP	0.182	

Table 5.8 Empirical AHP Result by IT

Ascending Priority	VPN Protocol	Weight	Respective
1	IP Security	0.598	Quality of Service
	L2TP	0.557	
	PPTP	0.309	
2	IP Security	0.583	Scalability
	L2TP	0.542	
	PPTP	0.300	
3	IP Security	0.518	Tunnelling and authentication
	L2TP	0.322	
	PPTP	0.204	
	IP Security	0.498	

4	L2TP	0.316	Remote Access
	PPTP	0.185	
5	IP Security	0.449	Operational costs reduction
	L2TP	0.324	
	PPTP	0.223	
6	IP Security	0.406	LAN Access
	L2TP	0.291	
	PPTP	0.187	

Table 5.9 Comparing the results between business and IT

Attribution	Information security feature definitions	Business		IT	
		Weight	Rank	Weight	Rank
1. Remote access	You are as travelling or home remote user access can gain access to company intranet from a wide range of locations including home.	0.537	3	0.507	4
2. Tunnelling and authentication	Establishment of data encrypted tunnel between your site and third parties (e.g. distributors, suppliers) and authenticates network user (identifying the user).	0.584	2	0.547	3
3. Operational costs reduction	VPN makes use of public network resources, business enterprise need not to buy its own networking equipment to cover remote user. Services costs less and deliver high-speed, secure connectivity to every branch location	0.598	1	0.452	5
4. Quality of service	The ability for VPN protocol to obtain the network service it requires for successful operation. VPN offer classes of service and quality of service (QoS) guarantee as the traffic remains within the domain of one network operator and the security afforded by traffic separation is comparable with traditional unencrypted solutions such as frame relay.	0.502	4	0.603	1
5. Scalability	A VPN platform should provide an upgrade path for supporting more users, as well as, for integrating new security services, such as virus protection and content filtering.	0.459	5	0.585	2
6. LAN access*	Using a dial-up line to connect a branch office to a corporate LAN. The VPN software uses the connection to the local ISP to create a VPN between	0.434		0.414	6

	the branch office router and the corporate hub router across the Internet.		6		

In table 5.9 shows result and compare the different between business and IT perspective on each attribution as their objective on Virtual Private Network (VPN). These results could sustain significant difference between business and IT objective (hypotheses 1).

Figure 5.1 to 5.6 used pyramid chart to view the graphical display of data, the legend explains the meaning of various colours on the chart, and the title indicates what the chart is used for. It can render a very effective result when analysing data of the same category on a defined scale.

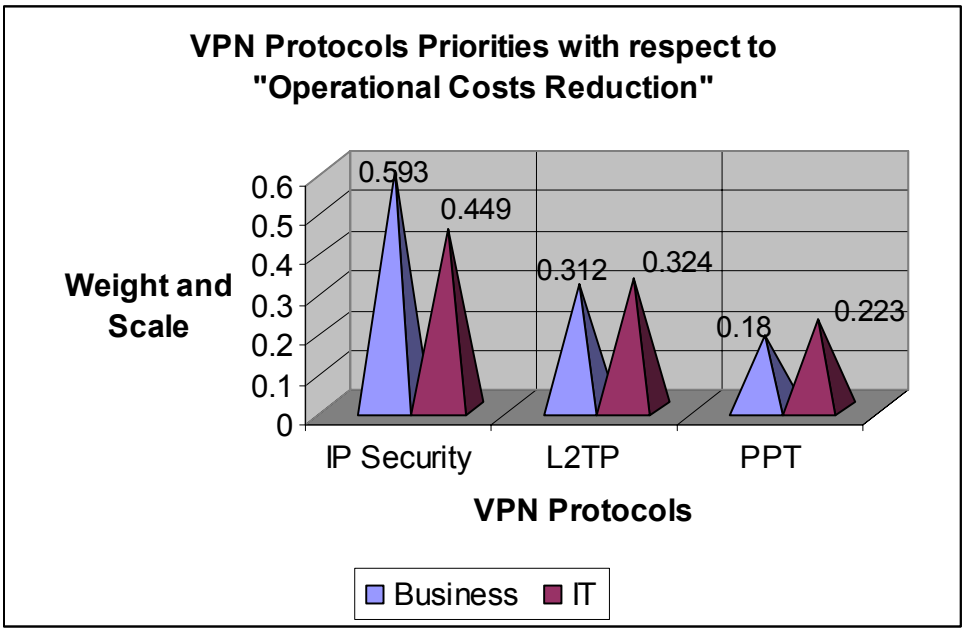

Figure 5.1 VPN protocols priorities with respect to "Operational Costs Reduction"

The pyramid chart in Figure 5.1 emphasizes high and low values each VPN protocol. It helps to compare items with respect to "Operational Costs Reduction". Business and IT had different perspective with respect to operational costs reduction. For example, business weighted IP security with respect to operational costs reduction at 0.593. IT gained only 0.449 and evaluated IP security less important than business executive. Business perceive operational costs reduction is important objective in their AHP ratio-scale as result because of VPN makes use of public network resources, business enterprise need not to buy its own networking equipment to cover remote user. A service costs less and delivers high-speed, secure connectivity to every branch location. In second, IT professional weighted L2TP with

respect to operational costs reduction at 0.324 which is higher than business executive (0.312). Based on this VPN protocols evaluation, there is significant different between business and IT objectives.

The pyramid chart, in figure 5.2, shows the different perspective between business and IT in each protocol. In figure 5.2, business weighted and compared IP security with respect to Tunnelling and Authentication at 0.575 as AHP ratio-scale. On another hand, IT gained only 0.518 at IP Security. In this VPN protocols evaluation,

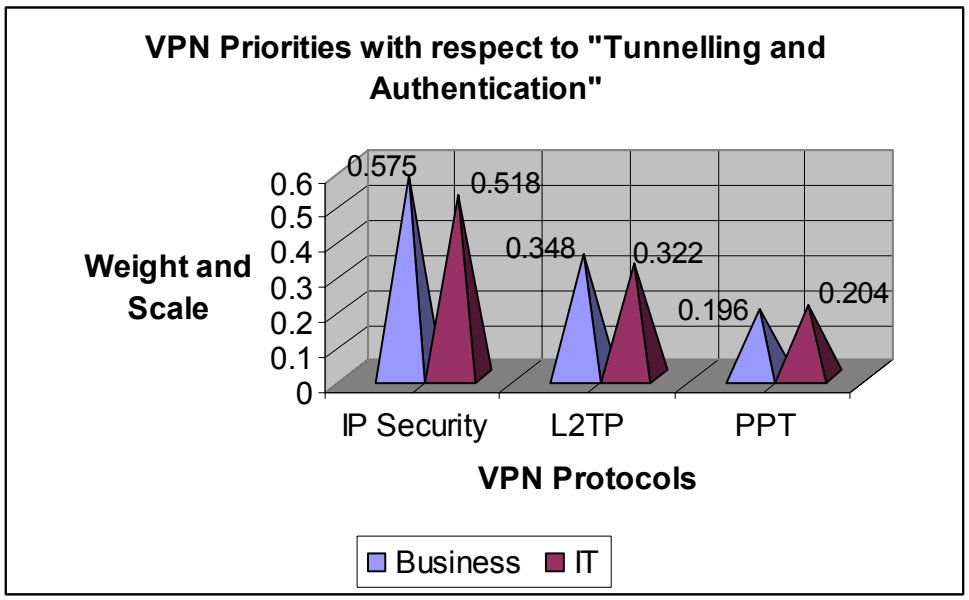

Figure 5.2 VPN protocols priorities with respect to "Tunnelling and Authentication"

business perceive tunnelling and authentication is important objective in their AHP ratio-scale as result because of establishment of data encrypted tunnel between their site and third parties (e.g. distributors, suppliers) and authenticates network user (identifying the user). It must also provide audit and accounting records to show who accessed what information and when.

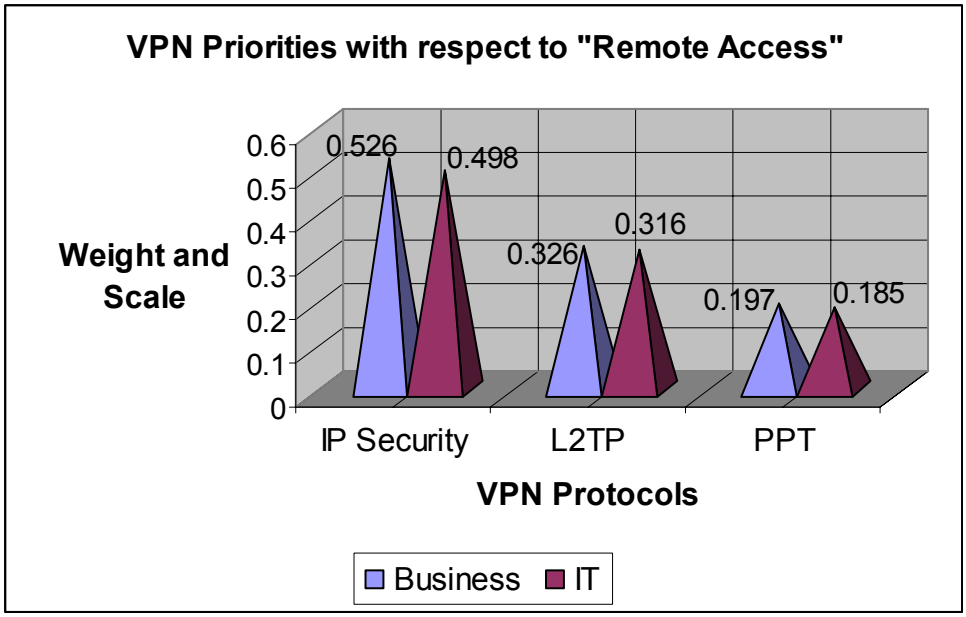

Figure 5.3 VPN protocols priorities with respect to "Remote Access"

The pyramid chart, in figure 5.3, shows the different perspective between business and IT in each protocol. In figure 5.3, business weighted and compared IP security with respect to Remote Access at 0.526 as AHP ratio-scale. On another hand, IT gained only 0.498 at IP Security. In this VPN protocols evaluation, both business and IT perceive remote access is important objective in their AHP ratio-scale as result because if they are as travelling or home remote user access can gain access to company intranet from a wide range of locations including home. The outcome of the analysis could advise IT objective can significantly improved business performance.

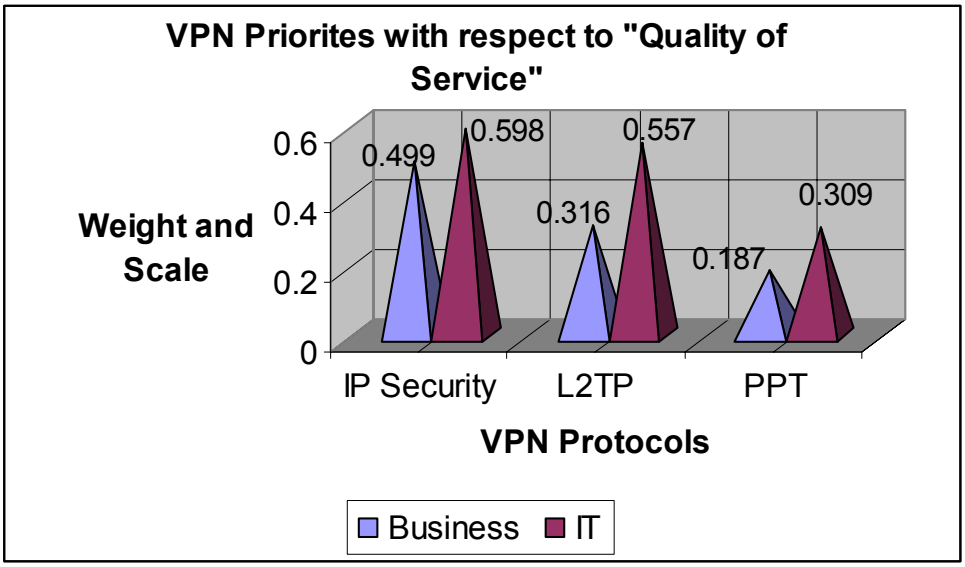

Figure 5.4 VPN protocols priorities with respect to "Quality of Service"

The pyramid chart, in figure 5.4, shows the different perspective between business and IT in each protocol. In figure 5.4, IT weighted and compared IP security with respect to Quality of Service at 0.598 as the first rank in AHP ratio-scale. Business gained only 0.499 at IP Security and rank number 4 (see table 5.7). In this VPN protocols evaluation, IT perceive quality of service is important objective in their AHP ratio-scale as result because the ability for VPN protocol to obtain the network service it requires for successful operation. VPN offer classes of service and quality of service (QoS) guarantee as the traffic remains within the domain of one network operator and the security afforded by traffic separation is comparable with traditional unencrypted solutions such as frame relay.

The pyramid chart, in figure 5.5, shows the different perspective between business and IT in each protocol. In figure 5.5, IT weighted and compared IP security with respect to Scalability at 0.583 and ranks number two in AHP ratio-scale (see table 5.7). Business gained only 0.452 at IP Security. In this VPN protocols evaluation, IT perceive scalability is important objective in their AHP ratio-scale as result because

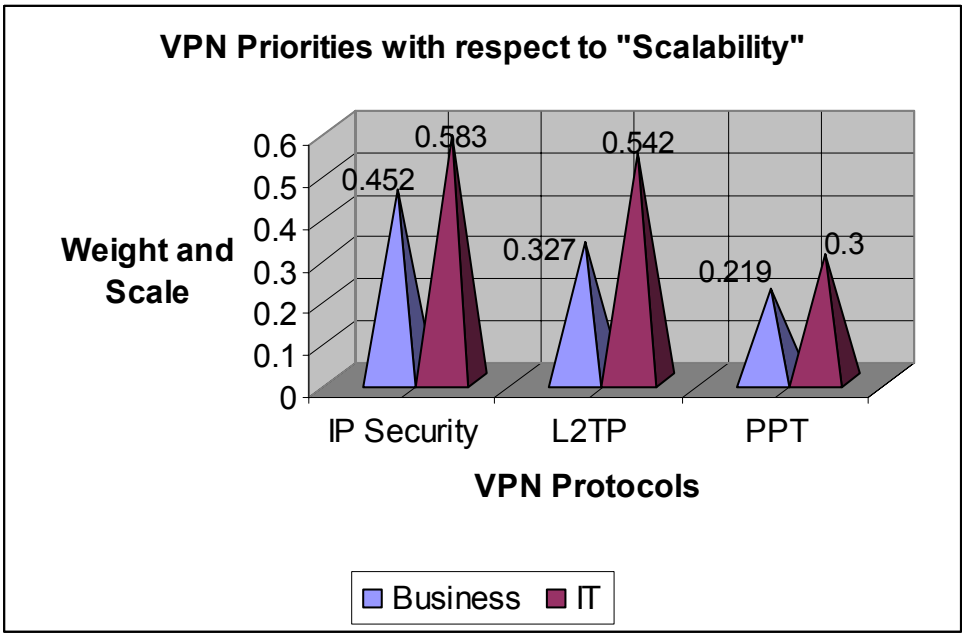

Figure 5.5 VPN protocols priorities with respect to "Scalability"

a VPN platform should provide an upgrade path for supporting more users, as well as, for integrating new security services, such as virus protection and content filtering. Business distinguished different from IT because Scalability was more in technique skill which allows IT people to upgrade VPN systems easier.

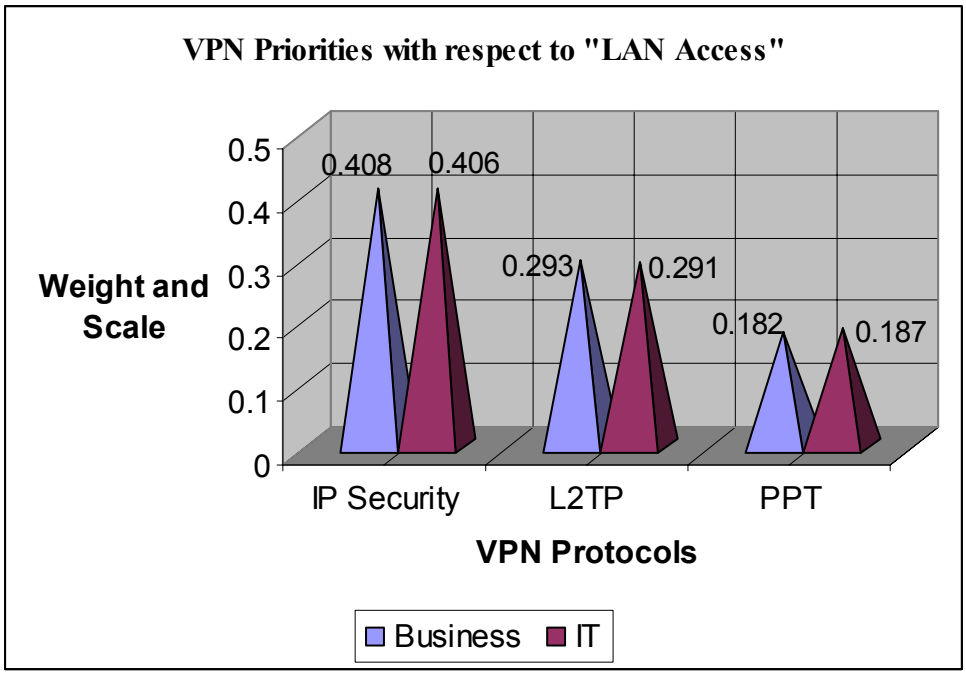

Figure 5.6 VPN protocols priorities with respect to "LAN Access"

The pyramid chart, in figure 5.6, shows the different perspective between business and IT in each protocol. In figure 5.6, business weighted and compared IP security with respect to LAN Access at 0.408. IT gained very much close to business which was 0.406 at IP Security. In this VPN protocols evaluation, business and IT perceive LAN access is important objective in their AHP ratio-scale as result because using a dial-up line to connect a branch office to a corporate LAN. The VPN software uses the connection to the local ISP (Internet Service Provide) to create a VPN between the branch office router and the corporate hub router across the Internet.

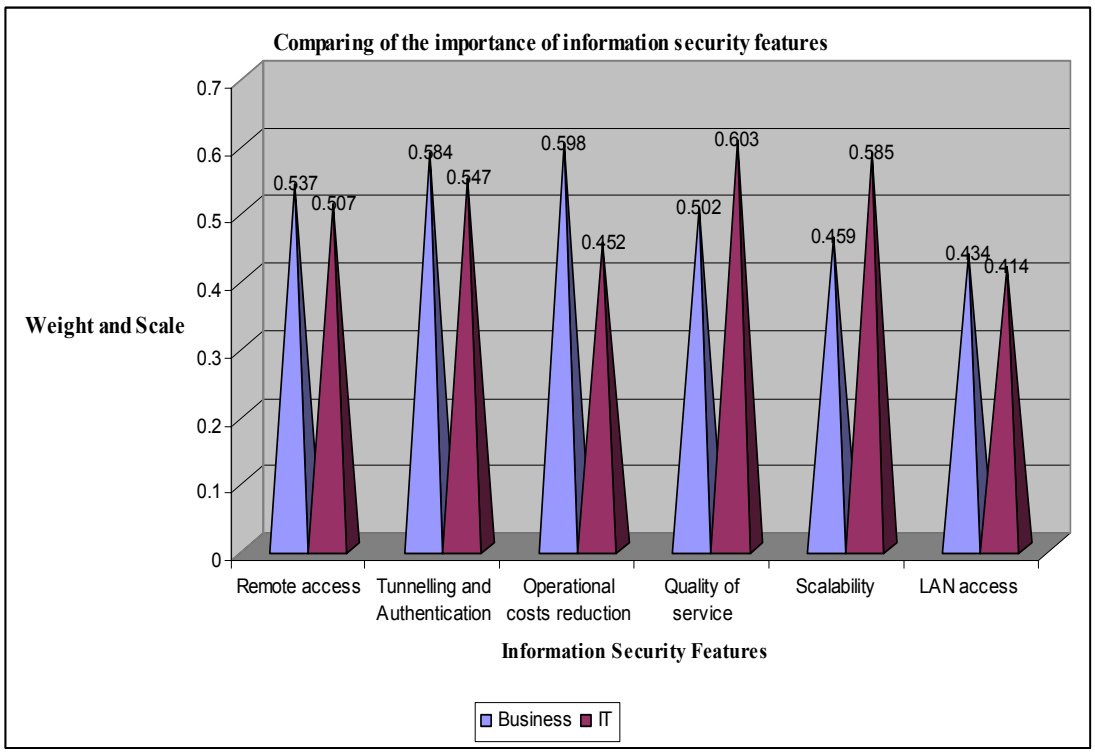

Figure 5.7 Comparing of the importance of information security features

In figure 5.7 used pyramid chart to show the result of information security features between business and IT. The overall priority for each alternative was obtained by summing the product of the criteria weight and the contribution of the alternative, with respect to the criterion. Obtain the final weights and ranking to the alternative with respect to the goal. Business people weighted more importance on “Operational costs reduction” as first priority at 0.598 and “LAN access” was last priority at 0.434. On other hand, IT people weighted

importance on “Quality of Service” as first priority at 0.603 and “LAN access” was last priority at 0.414.

5.1.6.3 Summary

In summary, this would distinguish the different perspective between business executive and IT professional of the organization structures their objectives in a hierarchic framework. AHP ratio-scale could illustrate business objective bias can significantly predict systems capability such as VPN security technology. The outcome of the analysis could advise IT objective can significantly improved business performance by using VPN system in their organizations. Tables as above sections of phase one represents results of the importance of information security features between business and IT including weighing and priority. In the result of phase one can be discussed and illustrated more detail in triangulation of data which comparing with phase two, and three as section 3.

5.1.7 Phase Two of Data Analysis

In this phase investigated and answered sub questions in section 3 of chapter 4 as following: (i) in what ways can a more efficient computer security system benefit the overall organisation competitive advantage? (ii) In what ways can the VPN improve the performance of the employees and managers in an organisation? (iii) What is the relationship between MIS security and competitive advantage? (iv) In what ways can VPN provide cost advantage? (v) What intangible MIS elements contribute to business value delivery? (vi) What organisational capabilities are enhanced by effective MIS security? Second Phase, data analysis included descriptive statistics including frequencies, means, medians, and standard deviations (see tables 5.10 and 5.11).

5.1.7.1 Research findings

Descriptive statistics were used to describe the basic features of the data in this study. They provide simple summaries about the sample and the measures on competitive advantage as descriptive in triangulation method. Together with simple graphics analysis, they form the basis of virtually every quantitative analysis of data. With descriptive statistics author could simply describing what was or what the data shows. Descriptive Statistics were used to present quantitative descriptions in a manageable form. Descriptive statistics help this study to simply large amounts of data in a sensible way. Each descriptive statistic reduces lots of data into a simpler summary.

In this study, the central tendency of a distribution is an estimate of the centre of a distribution of values including mean, median, and standard deviation. The Mean or average

is probably the most commonly used method of describing central tendency. The Median is the score found at the exact middle of the set of values. The Standard Deviation is a more accurate and detailed estimate of dispersion because an outlier can greatly exaggerate the range. The Standard Deviation shows the relation that set of scores has to the mean of the sample.

In tables 5.10 shows overall of the sample and the measures on competitive advantage as descriptive in phase two, which contains details constructs in columns including competitive advantage questions, mean, median, standard deviation (STDEV).

Table 5.10 over all of sample and measures on competitive advantage

Question	Mean	Median	STDEV
Question 1	1.577	2	0.5038
	1.591	2	0.5032
Question 2	3.846	4	0.6748
	3.773	4	0.5284
Question 3	3.885	4	0.6528
	3.864	4	0.7102
Question 4	3.962	4	0.6622
	4.091	4	0.6838
Question 5	3.654	4	0.6288
	3.733	4	0.6853
Question 6	3.923	4	0.5602
	4.182	4	0.5885
Question 7	3.808	4	0.6939
	3.864	4	0.7102
Question8	3.731	4	0.5335
	3.818	4	0.5885
Question 9	3.808	4	0.6337
	3.955	4	0.6530
Question 10	3.462	3	0.6469
	3.591	3	0.7341
Question 11	4.154	4	0.6748
	4.000	4	0.6901
Question 12	3.654	4	0.4852
	3.591	4	0.5903
Question 13	4.192	4	0.7494
	4.045	4	0.8439
Question 14	4.115	4	0.7656
	4.00	4	0.8165
Question 15	4.077	4	0.7961
	3.727	4	0.7673
Question 16	4.538	5	2.1969
	4.409	5	0.7341
Question 17	4.615	5	0.5711
	4.591	5	0.5903

5.1.7.2 Business and IT Finding

The results for competitive advantage questions 1 -17 are displayed in Table 5.11 (standard deviation) and 5.12 (mean and median) for both business and IT. Although both the mean and median of the performance measures are reported for both samples, the medians are considered to be better indicators. The Means procedure calculates subgroup means and related univariate statistics for dependent variables within categories of one or more independent variables. The results table 5.12 displays the default statistics for sections at each questionnaire which responded by business and IT people. Across all rows of the table 5.12, the mean column shows how average questionnaire differs by business and IT within level of sections. Finally, the Std. Deviation column indicates that some respond by IT people varies more widely than business people. Estimates standard deviation based on a sample. The standard deviation is a measure of how widely values are dispersed from the average value (the mean).

Table 5.11 Competitive advantage questionnaires both business and IT: Standard Deviation

Construct	Item/Question	Business	IT
		STDEV	STDEV
Section One VPN Implementation Before/After	1. indicate how you compared with your competitors with regard to the use of information security technology for competitive advantage "before" the implementation of Virtual Private Network	0.5038	0.5032
	2. indicate how you compared with your competitors with perdition to the use of information security technology for competitive advantage "after "the implementation of Virtual Private Network	0.6748	0.5284
Section Two It's essential to exchange information quickly and reliably with customers, suppliers and business partners. Your company document exchange online tools enable companies to easily and safely exchange important even confidential	3. Save yourself the time and cost of sending documents via overnight or fax	0.6528	0.7102
	4**.** Limit incompatibility so important documents can be read, re-sent or printed as needed	0.6622	0.6838
	5. Protect your privacy via encryption and password-only access	0.6288	0.6853
	6. Move unusually large files without computer networking restrictions	0.5602	0.5885
	7. Monitor the digital delivery of your documents with instant receipt notification	0.6939	0.7102
	8. A high degree of reliability because of the service's redundancies and backup systems	0.5335	0.5885
	9. More information available for customer verification of product delivery and receipt	0.6337	0.6530

information over the Internet.	10. Customized reports about your customers and products	0.6469	0.7341
	11. Improved accuracy; elimination of illegible handwritten records	0.6748	0.6901
Section Three information security capabilities that contributed to the successful implementation of your organization chosen Virtual Private Network (VPN) enhancement	12. Your organizations ability to develop and experiment with VPN, which enable business processing and performance to take advantage of VPN and trends	0.4852	0.5903
	13. Your organization's ability to share information throughout the organization through effective VPN and improve business competitive advantage on this VPN system	0.7494	0.8439
	14. The ability of your MIS department to understand and use VPN for security and protection	0.7656	0.8165
	15. Your organizations ability to anticipate future changes and growth as perditions in VPN system capability, to choose information security technology that can accommodate this change and to efficiently mange the resulting information security technology change and growth	0.7961	0.7673
	16. Your organization's IT ability to ensure business performance and MIS strategies are integrated with organizational functional plans and MIS align with organizational needs	2.1969	0.7341
	17. Your MIS security ability to gain competitive advantage and secure information systems in organization	0.5711	0.5903

Table 5.12 Competitive advantage questionnaires both business and IT: Mean and Median

Construct	**Item/Question**	**Business**		**IT**	
		Mean	Median	Mean	Median
Section One VPN Implementation Before/After	1. indicate how you compared with your competitors with regard to the use of information security technology for competitive advantage "before" the implementation of Virtual Private Network	1.577	2	1.591	2
	2. indicate how you compared with your competitors with perdition to the use of information security technology for competitive advantage "after "the implementation of Virtual Private Network	3.846	4	3.773	4

Section Two It's essential to exchange information quickly and reliably with customers, suppliers and business partners. Your company document exchange online tools enable companies to easily and safely exchange important even confidential information over the Internet.	3. Save yourself the time and cost of sending documents via overnight or fax	3.885	4	3.864	4
	4**.** Limit incompatibility so important documents can be read, re-sent or printed as needed	3.962	4	4.091	4
	5. Protect your privacy via encryption and password-only access	3.654	4	3.733	4
	6. Move unusually large files without computer networking restrictions	3.923	4	4.182	4
	7. Monitor the digital delivery of your documents with instant receipt notification	3.808	4	3.864	4
	8. A high degree of reliability because of the service's redundancies and backup systems	3.731	4	3.818	4
	9. More information available for customer verification of product delivery and receipt	3.808	4	3.955	4
	10. Customized reports about your customers and products	3.462	3	3.591	3
	11. Improved accuracy; elimination of illegible handwritten records	4.154	4	4.000	4
Section Three information security capabilities that contributed to the successful implementation of your organization chosen Virtual Private Network (VPN) enhancement	12. Your organizations ability to develop and experiment with VPN, which enable business processing to take advantage of VPN and trends	3.654	4	3.591	4
	13. Your organization's ability to share information throughout the organization through effective VPN and improve business competitive advantage on this VPN system	4.192	4	4.045	4
	14. The ability of your MIS department to understand and use VPN for security and protection	4.115	4	4.00	4
	15. Your organizations ability to anticipate future changes and growth as perditions in VPN system capability, to choose information security technology that can accommodate this change and to efficiently mange the resulting information security technology change and growth	4.077	4	3.727	4

	16. Your organization's IT ability to ensure business performance and MIS strategies are integrated with organizational functional plans and MIS align with organizational needs	4.538	5	4.409	5
	17. Your MIS security ability to gain competitive advantage and secure information systems in organization	4.615	5	4.591	5

In tables 5.13– 5.29 (business) and 5.30 – 5.46 (IT) used the frequencies procedure to provide statistics that are useful for describing type of variable. The Frequencies procedure is useful for obtaining summaries of individual variables. The frequency tables 5.13 – 5.29 show the precise frequencies for each category.

Table 5.13 Frequency competitive advantage question # 1: Business respondents

Competitive Advantage Question # 1

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly disagree	11	42.3	42.3	42.3
	disagree	15	57.7	57.7	100.0
	Total	26	100.0	100.0	

In question 1, business responded in section 1 of questionnaire on "Please use scale as below to indicate how you compared with your competitors with regard to the use of information security technology for competitive advantage "**before"** the implementation of Virtual Private Network". In this question, business people, as respondents, need to think about if their organization was secure and gain competitive advantage between competitors. In table 5.13, the frequency column reported that 11 of business respondent came from "strongly disagree" (1-5 Likert response scale). This was equivalent to 42.3 percent of total number of business respondents. There were 15 of business respondent came from "disagree" or equivalent to 57.7 percent. Both of 11 (strongly disagree) and 15 (disagree) of IT respondent didn't think their organizations gain competitive advantage on information security technology when comparing with competitors because there was no information security technology existing in their organization in the past.

In summary, there was no significantly effective information security system before the implementation of Virtual Private Network in their organization. The result in this question could notify that their organization did not gain any competitive advantage.

Table 5.14 Frequency competitive advantage question # 2: Business respondents

Competitive Advantage Question # 2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	8	30.8	30.8	30.8
	agree	14	53.8	53.8	84.6
	strongly agree	4	15.4	15.4	100.0
	Total	26	100.0	100.0	

In question 2, business responded in section 1 of questionnaire on "Please use scale as below to indicate how you compared with your competitors with prediction to the use of information security technology for competitive advantage "**after"** the implementation of Virtual Private Network". In this question, business people, as respondents, need to think about if their organization was secure and gain competitive advantage between competitors. In table 5.14, the frequency column reported that 14 of business respondent came from "agree" (1-5 Likert response scale). This was equivalent to 53.8 percent of total number of business respondents. There were 4 of business respondent came from "strongly agree" or equivalent to 15.4 percent. Both of 14 (agree) and 4 (strongly agree) of business people believed that after their organization implemented Virtual Private Network. Their organization gain competitive advantage and information systems are secure and safe. Other 8 of business respondent did "not sure" if their organization could gain competitive advantage after the implementation of VPN. In this question 2, there were insignificantly "strongly agree" and "agree' more than "not sure" in Likert response scale which business compensated concentration on the improvement and gain competitive advantage after the implementation of VPN as their perdition of VPN implementation. Business executive could distinguish the different after the implementation of VPN. The result from this question 2 could verify that the variation business objectives can significantly predict system capability (Hypotheses 6) such as implementation of VPN.

Table 5.15 Frequency competitive advantage question # 3: Business respondents

Competitive Advantage Question # 3

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	7	26.9	26.9	26.9
	agree	15	57.7	57.7	84.6
	strongly agree	4	15.4	15.4	100.0
	Total	26	100.0	100.0	

In question 3, business people responded in section 2 of questionnaire was about their

company document exchange online tools enable companies to easily and safely exchange important even confidential information over the Internet. With their document exchange customers can comfortably send and receive critical business documents and other information forms like video, audio and text via the Internet and have full control over their digitally delivered documents. The question focused on "Save themself the time and cost of sending documents via overnight or fax". In table 5.15 the frequency column reported that 15 of business respondent came from "agree" and it was equivalent to 57.7 %. There were 4 of them chose "strongly agree" and it was equivalent to 15.4 %. Both 15 and 4 of business respondent believed that they can save the time and cost of sending document via overnight. Other 7 of business respondent did "not sure" if they can save the time and cost of sending document via overnight.

In summary, there were significantly "strongly agree" and "agree" more than disagree which this question could sustain MIS security can significantly predict

Table 5.16 Frequency competitive advantage question # 4: Business respondents

Competitive Advantage Question # 4

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	6	23.1	23.1	23.1
	agree	15	57.7	57.7	80.8
	strongly agree	5	19.2	19.2	100.0
	Total	26	100.0	100.0	

organization competitive advantage (Hypotheses 7).

In question 4, business people responded in section 2 of questionnaire was about their company document exchange online tools enable companies to easily and safely exchange important even confidential information over the Internet. With their document exchange customers can comfortably send and receive critical business documents and other information forms like video, audio and text via the Internet and have full control over their digitally delivered documents. It focused on "Limit incompatibility so important documents can be read, re-sent or printed as needed". In table 5.16, the frequency column reported that 15 of business respondent came from "agree" or equivalent to 57.7 percent. There were 5 of them chose "strongly agree" or equivalent to 19.2 percent. Both 15 (agree) and 5 (strongly agree) of business respondent believed and supported the question on "Limit incompatibility so important documents can be read, re-sent or printed as needed". Other 6 of business

respondent did “not sure” about “Limit incompatibility so important documents can be read, re-sent or printed as needed”.

In summary, there were significantly “strongly agree” and “agree”more than disagree which this question could sustain MIS security can significantly predict organization competitive advantage (Hypotheses 7).

Table 5.17 Frequency competitive advantage question # 5: Business respondents

Competitive Advantage Question # 5

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	11	42.3	42.3	42.3
	agree	13	50.0	50.0	92.3
	strongly agree	2	7.7	7.7	100.0
	Total	26	100.0	100.0	

In question 5, business people responded in section 2 of questionnaire was about their company document exchange online tools enable companies to easily and safely exchange important even confidential information over the Internet. With their document exchange customers can comfortably send and receive critical business documents and other information forms like video, audio and text via the Internet and have full control over their digitally delivered documents. The question focused on “Protect their privacy via encryption and password-only access”. In table 5.17, the frequency column reported that 13 of business respondent came from “agree” and it was equivalent to 50.0 %. There were 2 of them chose “strongly agree” and it was equivalent to 7.7 %. Both 15 (agree) and 5 (strongly agree) of business respondent believed and supported the question on “Protect their privacy via encryption and password-only access”. Other 11 of business respondent did “not sure” about protect their privacy via encryption and password-only access. In summary, there were significantly “strongly agree” and “agree” more than disagree which this question could sustain MIS security can significantly predict organization competitive advantage (Hypotheses 7).

Table 5.18 Frequency competitive advantage question # 6: Business respondents

Competitive Advantage Question # 6

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	5	19.2	19.2	19.2

	agree	18	69.2	69.2	88.5
	strongly agree	3	11.5	11.5	100.0
	Total	26	100.0	100.0	

In question 6, business people responded in section 2 of questionnaire was about their company document exchange online tools enable companies to easily and safely exchange important even confidential information over the Internet. With their document exchange customers can comfortably send and receive critical business documents and other information forms like video, audio and text via the Internet and have full control over their digitally delivered documents. The question focused on "Move unusually large files without computer networking restrictions". In table 5.18, the frequency column reported that 18 of business respondent came from "agree" and it was equivalent to 69.2 %. There were 3 of them chose "strongly agree" and it was equivalent to 11.5 %. Both 18 (agree) and 3 (strongly agree) of business respondent believed that they can move unusually large files without computer networking restrictions. Other 5 of business respondent did "not sure" if they can move unusually large files without computer networking restrictions.

In summary, there were significantly "strongly agree" and "agree" more than disagree which this question could sustain MIS security can significantly predict organization competitive advantage (Hypotheses 7).

Table 5.19 Frequency competitive advantage question # 7: Business respondents

Competitive Advantage Question # 7

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	9	34.6	34.6	34.6
	agree	13	50.0	50.0	84.6
	strongly agree	4	15.4	15.4	100.0
	Total	26	100.0	100.0	

In question 7, business people responded in section 2 of questionnaire was about their company document exchange online tools enable companies to easily and safely exchange important even confidential information over the Internet. With their document exchange customers can comfortably send and receive critical business documents and other information forms like video, audio and text via the Internet and have full control over their digitally delivered documents. The question focused on "Monitor the digital delivery of their documents with instant receipt notification". In table 5.19, the frequency column reported

that 13 of business respondent came from “agree” and it was equivalent to 50.0 %. There were 4 of them chose “strongly agree” and it was equivalent to 15.4 %. Both 13 (agree) and 4 (strongly agree) of business respondent believed and supported question on “Monitor the digital delivery of their documents with instant receipt notification”. Other 9 of business respondent did “not sure” on “Monitor the digital delivery of their documents with instant receipt notification”.

In summary, there were significantly “strongly agree” and “agree” more than disagree which this question could sustain MIS security can significantly predict organization competitive advantage (Hypotheses 7).

Table 5.20 Frequency competitive advantage question # 8: Business respondents

Competitive Advantage Question # 8

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	8	30.8	30.8	30.8
	agree	17	65.4	65.4	96.2
	strongly agree	1	3.8	3.8	100.0
	Total	26	100.0	100.0	

In question 8, business people responded in section 2 of questionnaire was about their company document exchange online tools enable companies to easily and safely exchange important even confidential information over the Internet. With their document exchange customers can comfortably send and receive critical business documents and other information forms like video, audio and text via the Internet and have full control over their digitally delivered documents. The question focused on “A high degree of reliability because of the service's redundancies and backup systems”. In table 5.20, the frequency column reported that 17 of business respondent came from “agree” and it was equivalent to 65.4 %. There was 1 of them chose “strongly agree” and it was equivalent to 3.8 %. Both 17 (agree) and 1 (strongly agree) of business respondent believed and supported question on “A high degree of reliability because of the service's redundancies and backup systems”. Other 8 of business respondent did “not sure” on “A high degree of reliability because of the service's redundancies and backup systems”.

In summary, there were significantly “strongly agree” and “agree” more than disagree which this question could sustain MIS security can significantly predict organization competitive advantage (Hypotheses 7).

Table 5.21 Frequency competitive advantage question # 9: Business respondents

Competitive Advantage Question # 9

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	8	30.8	30.8	30.8
	agree	15	57.7	57.7	88.5
	strongly agree	3	11.5	11.5	100.0
	Total	26	100.0	100.0	

In question 9, business people responded in section 2 of questionnaire was about their company document exchange online tools enable companies to easily and safely exchange important even confidential information over the Internet. With their document exchange customers can comfortably send and receive critical business documents and other information forms like video, audio and text via the Internet and have full control over their digitally delivered documents. The question focused on "More information available for customer verification of product delivery and receipt". In table 5.21, the frequency column reported that 15 of business respondent came from "agree" and it was equivalent to 57.7 %. There were 3 of them chose "strongly agree" and it was equivalent to 11.5 %. Both 15 (agree) and 3 (strongly agree) of business respondent believed and supported question on "More information available for customer verification of product delivery and receipt". Other 8 of business respondent did "not sure" about "More information available for customer verification of product delivery and receipt".

In summary, there were significantly "strongly agree" and "agree" more than disagree which this question could sustain MIS security can significantly predict organization competitive advantage (Hypotheses 7).

Table 5.22 Frequency competitive advantage question # 10: Business respondents

Competitive Advantage Question # 10

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	16	61.5	61.5	61.5
	agree	8	30.8	30.8	92.3
	strongly agree	2	7.7	7.7	100.0
	Total	26	100.0	100.0	

In question 10, business people responded in section 2 of questionnaire was about their company document exchange online tools enable companies to easily and safely exchange important even confidential information over the Internet. With their document exchange

customers can comfortably send and receive critical business documents and other information forms like video, audio and text via the Internet and have full control over their digitally delivered documents. The question focused on "Customized reports about their customers and products". In table 5.22, the frequency column reported that 8 of business respondent came from "agree" and it was equivalent to 30.8 %. There were 2 of them chose "strongly agree" and it was equivalent to 7.7 %. Both 8 (agree) and 2 (strongly agree) of business respondent believed and supported question on "Customized reports about their customers and products". Other 16 of business respondent came from "not sure" on this question 10.

In summary, there were significantly "strongly agree" and "agree"more than disagree which this question could sustain MIS security can significantly predict organization competitive advantage (Hypotheses 7).

Table 5.23 Frequency competitive advantage question # 11: Business respondents

Competitive Advantage Question # 11

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	4	15.4	15.4	15.4
	agree	14	53.8	53.8	69.2
	strongly agree	8	30.8	30.8	100.0
	Total	26	100.0	100.0	

In question 11, business people responded in section 2 of questionnaire was about their company document exchange online tools enable companies to easily and safely exchange important even confidential information over the Internet. With their document exchange customers can comfortably send and receive critical business documents and other information forms like video, audio and text via the Internet and have full control over their digitally delivered documents. The question focused on "Improved accuracy; elimination of illegible handwritten records". In table 5.23, the frequency column reported that 14 of business respondent came from "agree" and it was equivalent to 53.8 %. There were 8 of them chose "strongly agree" and it was equivalent to 30.8 %. Both 14 (agree) and 8 (strongly agree) of business respondent believed and supported question on "Improved accuracy; elimination of illegible handwritten records". Other 4 of business respondent came from "not sure" about "Improved accuracy; elimination of illegible handwritten records".

In summary, there were significantly "strongly agree" and "agree" more than disagree which this question could sustain MIS security can significantly predict organization competitive

advantage (Hypotheses 7).

Table 5.24 Frequency competitive advantage question # 12: Business respondents

Competitive Advantage Question # 12

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	9	34.6	34.6	34.6
	agree	17	65.4	65.4	100.0
	Total	26	100.0	100.0	

In question 12, business people responded in section 3 of questionnaire on "Their organizations ability to develop and experiment with VPN, which enable business processing and performance to take advantage of VPN and trends". In table 5.24, the frequency column reported that 17 of business respondent came from "agree" and it was equivalent to 65.4 %. This responds of business can be supported the hypothesis on "VPN usage has significant effect on business processing" because these 17 of business respondent believed that their organizations ability to develop and experiment with VPN, which enable business processing and performance to take advantage of VPN and trends. Other 9 of business respondent did "not sure" if their organizations ability to develop and experiment with new technologies, which enable they to take advantage of emerging technologies and trends or not.

In this question, there was significantly "agree" more than "not sure" as Likert response scale which business compensated concentration on their organizations ability to develop and experiment with VPN, which enable business processing and performance to take advantage of VPN and trends. The result from these business respondents could provide evidence and sustain that VPN usage has a significantly effect on business competitive advantage (Hypotheses 2).

Table 5.25 Frequency competitive advantage question # 13: Business respondents

Competitive Advantage Question # 13

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	5	19.2	19.2	19.2
	agree	11	42.3	42.3	61.5
	strongly agree	10	38.5	38.5	100.0
	Total	26	100.0	100.0	

In question 13, business people responded in section 3 of questionnaire on "Their organization's ability to share information throughout the organization through effective VPN and improve business competitive advantage on this VPN system". In table 5.25, the

frequency column reported that 11 of business respondent came from "agree" and it was equivalent to 42.3 %. There were 10 of them chose "strongly agree" and it was equivalent to 38.5 %. Both 11 (agree) and 10 (strongly agree) of business respondent believed that their organization's ability to share information throughout the organization through effective VPN and communication platforms. Other 5 of business respondent did "not sure" if their organization's ability to share information throughout the organization through effective VPN and communication platforms.

In summary, there were significantly "strongly agree" and "agree" more than "not sure" as Likert response scale which business compensated concentration on their organization's ability to share information throughout the organization through effective VPN and improve business competitive advantage on this VPN system. The result from these business respondents could provide evidence and sustain that VPN usage has a significantly effect on business competitive advantage (Hypotheses 2).

Table 5.26 Frequency competitive advantage question # 14: Business respondents

Competitive Advantage Question # 14

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	6	23.1	23.1	23.1
	agree	11	42.3	42.3	65.4
	strongly agree	9	34.6	34.6	100.0
	Total	26	100.0	100.0	

In question 14, business people responded in section 3 of questionnaire on "The ability of their MIS department to understand and use VPN for security and protection". In table 5.26, the frequency column reported that 11 of business respondent came from "agree" and it was equivalent to 42.3 %. There were 9 of them chose "strongly agree" and it was equivalent to 34.6 %. This responds of business can be supported the hypothesis on "VPN usage has significant effect on MIS protection" because both 11 (agree) and 10 (strongly agree) of business respondent believed that the ability of their MIS department to understand and use VPN for security and protection. Other 6 of business respondent did "not sure" about this question.

In summary, there were significantly "strongly agree" and "agree" more than "not sure" as Likert response scale which business compensated concentration on the ability of their MIS department to understand and use VPN for security and protection. The result from these

business respondents could provide evidence and sustain that VPN usage has a significantly effect on MIS protection (Hypotheses 3).

In question 15, business people responded in section 3 of questionnaire on "Their organizations ability to anticipate future changes and growth as perditions in VPN system capability, to choose information security technology that can accommodate this change,

Table 5.27 Frequency competitive advantage question # 15: Business respondents

Competitive Advantage Question # 15

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	7	26.9	26.9	26.9
	agree	10	38.5	38.5	65.4
	strongly agree	9	34.6	34.6	100.0
	Total	26	100.0	100.0	

and to efficiently mange the resulting technology change and growth". In table 5.27, the frequency column reported that 10 of business respondent came from "agree" and it was equivalent to 38.5 %. There were 9 of them chose "strongly agree" and it was equivalent to 34.6 %. Both 10 (agree) and 9 (strongly agree) of business respondent believed that their organizations ability to anticipate future changes and growth, to chose information security technology that can accommodate this change and to efficiently mange the resulting technology change and growth. Other 7 of business respondent did "not sure" if their organizations ability to anticipate future changes and growth, to chose information security technology that can accommodate this change and to efficiently mange the resulting technology change and growth or not.

In summary, there were insignificantly "strongly agree" and "agree' more than "not sure" in Likert response scale which business compensated concentration on their organizations ability to anticipate future changes and growth as perditions in VPN system capability, to chose information security technology that can accommodate this change and to efficiently mange the resulting technology change and growth. Business executive could distinguish the different after the implementation of VPN. The result from this question 15 could verify that the variation business objectives can significantly predict system capability (Hypotheses 6) such as implementation of VPN.

Table 5.28 Frequency competitive advantage question # 16: Business respondents

Competitive Advantage Question # 16

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	1	3.8	3.8	3.8
	agree	10	38.5	38.5	42.3
	strongly agree	15	57.7	57.7	100.0
	Total	26	100.0	100.0	

In question 16, business people responded in section 3 of questionnaire on "Their organization's IT ability to ensure business performance and IS strategies are integrated with organizational functional plans and IS align with organizational needs".In table 5.28, the frequency column reported that 10 of business respondent came from "agree" and it was equivalent to 38.5 %. There were 15 of them chose "strongly agree" and it was equivalent to 57.7 %. This responds of business can be supported the hypothesis on "IT objective can significantly improve business performance" because both 10 (agree) and 15 (strongly agree) of business respondent believed that their organization's IT ability to ensure business performance and IS strategies are integrated with organizational functional plans and IS align with organizational needs. There was only 1 of business respondent did "not sure" if their organization's IT ability to ensure business performance and IS strategies are integrated with organizational functional plans and IS align with organizational needs.

Table 5.29 Frequency competitive advantage question # 17: Business respondents

Competitive Advantage Question # 17

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	1	3.8	3.8	3.8
	agree	8	30.8	30.8	34.6
	strongly agree	17	65.4	65.4	100.0
	Total	26	100.0	100.0	

In question 17, business people responded in section 3 of questionnaire on "Their MIS security ability to gain competitive advantage and secure information system in organization". In table 5.29, the frequency column reported that 8 of business respondent came from "agree" and it was equivalent to 30.8 %. There were 17 of them chose "strongly agree" and it was equivalent to 65.4 %. This responds of business can be supported the hypothesis on "MIS security can significantly predict organizational competitive advantage"

because both of 8 (agree) and 17 (strongly agree) of business respondent believed that their MIS security ability to gain competitive advantage and secure information system in organization. There was only 1 of business respondent came from "not sure" if their MIS security ability to gain competitive advantage and secure information system in organization or not.

In summary, there were insignificantly "strongly agree" and "agree' more than "not sure" in Likert response scale which business compensated concentration on their MIS security ability to gain competitive advantage and secure information system in organization. Business executive could distinguish the different after the implementation of VPN. The result from this question 17 could verify that MIS security can significantly predict organisational competitive advantage (Hypotheses 7).

In tables 5.30 – 5.46 (IT) used the frequencies procedure to provide statistics that are useful for describing type of variable. The Frequencies procedure is useful for obtaining summaries of individual variables. The frequency tables show the precise frequencies for each category.

Table 5.30 Frequency competitive advantage question # 1: IT respondents

Competitive Advantage Question # 1

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly disagree	9	34.6	40.9	40.9
	disagree	13	50.0	59.1	100.0
	Total	22	84.6	100.0	
Missing	System	4	15.4		
Total		26	100.0		

In question 1, IT responded in section 1 of questionnaire on "Please use scale as below to indicate how you compared with your competitors with regard to the use of information security technology for competitive advantage "**before"** the implementation of Virtual Private Network". In this question, IT people, as respondents, need to think about if their organization was secure and gain competitive advantage between competitors. In table 5.30, the frequency column reported that 9 of IT respondent came from "strongly disagree" (1-5 Likert response scale). This was equivalent to 34.6 percent of total number of business respondents. There were 13 of IT respondent came from "disagree" or equivalent to 50.0 percent. Both of 9 (strongly disagree) and 13 (disagree) of business respondent didn't think their organizations gain competitive advantage on information security technology when

comparing with competitors because there was no information security technology existing in their organization in the past.

Table 5.31 Frequency competitive advantage question # 2: IT respondents

Competitive Advantage Question # 2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	6	23.1	27.3	27.3
	agree	15	57.7	68.2	95.5
	strongly agree	1	3.8	4.5	100.0
	Total	22	84.6	100.0	
Missing	System	4	15.4		
Total		26	100.0		

In summary, there was no significantly effective information security system before the implementation of Virtual Private Network in their organization. The result in question 1 could notify that did not gain any competitive advantage.

In question 2, IT responded in section 1 of questionnaire on "Please use scale as below to indicate how you compared with your competitors with regard to the use of information security technology for competitive advantage "**after"** the implementation of Virtual Private Network". In this question, IT people, as respondents, need to think about if their organization was secure and gain competitive advantage between competitors after the implementation of VPN. In table 5.31, the frequency column reported that 15 of IT respondent came from "agree" (1-5 Likert response scale). This was equivalent to 57.7 percent of total number of IT respondents. There was 1 of IT respondent came from "strongly agree" or equivalent to 3.8 percent. Both of 15 (agree) and 1 (strongly agree) of business people believed that after their organization implemented Virtual Private Network. Their organization gain competitive advantage and information systems are secure and safe. Other 6 of business respondent did "not sure" if their organization could gain competitive advantage after the implementation of VPN.

In summary, there were insignificantly "strongly agree" and "agree' more than "not sure" in Likert response scale which IT compensated concentration on the improvement and gain competitive advantage after the implementation of VPN as their perdition of VPN implementation. IT professional could distinguish the different after the implementation of VPN. The result from this question 2 could verify that the variation business objectives can significantly predict system capability (Hypotheses 6) such as implementation of VPN.

Table 5.32 Frequency competitive advantage question # 3: IT respondents

Competitive Advantage Question # 3

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	7	26.9	31.8	31.8
	agree	11	42.3	50.0	81.8
	strongly agree	4	15.4	18.2	100.0
	Total	22	84.6	100.0	
Missing	System	4	15.4		
Total		26	100.0		

In question 3, IT responded in section 2 of questionnaire was about their company document exchange online tools enable companies to easily and safely exchange important even confidential information over the Internet. With their document exchange customers can comfortably send and receive critical business documents and other information forms like video, audio and text via the Internet and have full control over their digitally delivered documents. The question focused on "Save themself the time and cost of sending documents via overnight or fax". In table 5.32 the frequency column reported that 11 of IT respondent came from "agree" and it was equivalent to 42.3 %. There were 4 of them chose "strongly agree" and it was equivalent to 15.4 %. Both 11 and 4 of IT respondent believed that they can save the time and cost of sending document via overnight. Other 7 of IT respondent did "not sure" if they can save the time and cost of sending document via overnight.

In summary, there were significantly "strongly agree" and "agree"more than disagree which this question could sustain MIS security can significantly predict organization competitive advantage (Hypotheses 7).

Table 5.33 Frequency competitive advantage question # 4: IT respondents

Competitive Advantage Question # 4

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	4	15.4	18.2	18.2
	agree	12	46.2	54.5	72.7
	strongly agree	6	23.1	27.3	100.0
	Total	22	84.6	100.0	
Missing	System	4	15.4		
Total		26	100.0		

In question 4, IT responded in section 2 of questionnaire was about their company document exchange online tools enable companies to easily and safely exchange important even

confidential information over the Internet. With their document exchange customers can comfortably send and receive critical business documents and other information forms like video, audio and text via the Internet and have full control over their digitally delivered documents. It focused on "Limit incompatibility so important documents can be read, re-sent or printed as needed". In table 5.33, the frequency column reported that 12 of IT respondent came from "agree" or equivalent to 46.2 percent. There were 6 of them chose "strongly agree" or equivalent to 23.1 percent. Both 15 (agree) and 5 (strongly agree) of business respondent believed and supported the question on "Limit incompatibility so important documents can be read, re-sent or printed as needed". Other 6 of IT respondent did "not sure" about "Limit incompatibility so important documents can be read, re-sent or printed as needed". In summary, there were significantly "strongly agree" and "agree" more than disagree which this question could sustain MIS security can significantly predict organization competitive advantage (Hypotheses 7).

In question 5, IT people responded in section 2 of questionnaire was about their company document exchange online tools enable companies to easily and safely exchange important even confidential information over the Internet. With their document exchange customers can comfortably send and receive critical business documents and other information forms like video, audio and text via the Internet and have full control

Table 5.34 Frequency competitive advantage question # 5: IT respondents

Competitive Advantage Question # 5

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	8	30.8	36.4	36.4
	agree	11	42.3	50.0	86.4
	strongly agree	3	11.5	13.6	100.0
	Total	22	84.6	100.0	
Missing	System	4	15.4		
Total		26	100.0		

over their digitally delivered documents. The question focused on "Protect their privacy via encryption and password-only access". In table 5.34, the frequency column reported that 11 of IT respondent came from "agree" and it was equivalent to 42.3 %. There were 3 of them chose "strongly agree" and it was equivalent to 11.5 %. Both 11 (agree) and 3 (strongly agree) of IT respondent believed and supported the question on "Protect their privacy via

encryption and password-only access". Other 8 of IT respondent did "not sure" about protect their privacy via encryption and password-only access.

In summary, there were significantly "strongly agree" and "agree" more than disagree which this question could sustain MIS security can significantly predict organization competitive advantage (Hypotheses 7).

Table 5.35 Frequency competitive advantage question # 6: IT respondents

Competitive Advantage Question # 6

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	2	7.7	9.1	9.1
	agree	14	53.8	63.6	72.7
	strongly agree	6	23.1	27.3	100.0
	Total	22	84.6	100.0	
Missing	System	4	15.4		
Total		26	100.0		

In question 6, IT people responded in section 2 of questionnaire was about their company document exchange online tools enable companies to easily and safely exchange important even confidential information over the Internet. With their document exchange customers can comfortably send and receive critical business documents and other information forms like video, audio and text via the Internet and have full control over their digitally delivered documents. The question focused on "Move unusually large files without computer networking restrictions". In table 5.35, the frequency column reported that 14 of IT respondent came from "agree" and it was equivalent to 53.8 percent. There were 6 of them chose "strongly agree" and it was equivalent to 23.1 percent. Both 14 (agree) and 6 (strongly agree) of IT respondent believed that they can move unusually large files without computer networking restrictions. Other 2 of IT respondent did "not sure" if they can move unusually large files without computer networking restrictions.

In summary, there were significantly "strongly agree" and "agree" more than disagree which this question could sustain MIS security can significantly predict organization competitive advantage (Hypotheses 7).

Table 5.36 Frequency competitive advantage question # 7: IT respondents

Competitive Advantage Question # 7

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	7	26.9	31.8	31.8
	agree	11	42.3	50.0	81.8
	strongly agree	4	15.4	18.2	100.0
	Total	22	84.6	100.0	
Missing	System	4	15.4		
Total		26	100.0		

In question 7, IT responded in section 2 of questionnaire was about their company document exchange online tools enable companies to easily and safely exchange important even confidential information over the Internet. With their document exchange customers can comfortably send and receive critical business documents and other information forms like video, audio and text via the Internet and have full control over their digitally delivered documents. The question focused on "Monitor the digital delivery of their documents with instant receipt notification". In table 5.36, the frequency column reported that 11 of IT respondent came from "agree" and it was equivalent to 42.3 %. There were 4 of them chose "strongly agree" and it was equivalent to 15.4 %. Both 11 (agree) and 4 (strongly agree) of IT respondent believed and supported question on "Monitor the digital delivery of their documents with instant receipt notification". Other 7 of IT respondent did "not sure" on "Monitor the digital delivery of their documents with instant receipt notification". In summary, there were significantly "strongly agree" and "agree" more than disagree which this question could sustain MIS security can significantly predict organization competitive advantage (Hypotheses 7).

In question 8, IT people responded in section 2 of questionnaire was about their company document exchange online tools enable companies to easily and safely exchange important even confidential information over the Internet. With their document exchange customers can comfortably send and receive critical business documents and other information forms like video, audio and text via the Internet and have full control over

Table 5.37 Frequency competitive advantage question # 8: IT respondents

Competitive Advantage Question # 8

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	6	23.1	27.3	27.3
	agree	14	53.8	63.6	90.9
	strongly agree	2	7.7	9.1	100.0
	Total	22	84.6	100.0	
Missing	System	4	15.4		
Total		26	100.0		

the digitally delivered documents. The question focused on "A high degree of reliability because of the service's redundancies and backup systems". In table 5.37, the frequency column reported that 14 of IT respondent came from "agree" and it was equivalent to 53.8 %. There were 2 of them chose "strongly agree" and it was equivalent to 3.8 %. Both 14 (agree) and 2 (strongly agree) of IT respondent believed and supported question on "A high degree of reliability because of the service's redundancies and backup systems". Other 6 of IT respondent did "not sure" about this question".

In summary, there were significantly "strongly agree" and "agree" more than disagree which this question could sustain MIS security can significantly predict organization competitive advantage (Hypotheses 7).

Table 5.38 Frequency competitive advantage question # 9: IT respondents

Competitive Advantage Question # 9

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	5	19.2	22.7	22.7
	agree	13	50.0	59.1	81.8
	strongly agree	4	15.4	18.2	100.0
	Total	22	84.6	100.0	
Missing	System	4	15.4		
Total		26	100.0		

In question 9, IT responded in section 2 of questionnaire was about their company document exchange online tools enable companies to easily and safely exchange important even confidential information over the Internet. With their document exchange customers can comfortably send and receive critical business documents and other information forms like video, audio and text via the Internet and have full control over their digitally delivered

documents. The question focused on “More information available for customer verification of product delivery and receipt”. In table 5.38, the frequency column reported that 13 of IT respondent came from “agree” and it was equivalent to 50.0 precent. There were 4of them chose “strongly agree” and it was equivalent to 15.4 %. Both 13 (agree) and 4 (strongly agree) of IT respondent believed and supported question on “More information available for customer verification of product delivery and receipt”. Other 5 of respondent did “not sure” about “More information available for customer verification of product delivery and receipt”.

In summary, there were significantly “strongly agree” and “agree” more than disagree which this question could sustain MIS security can significantly predict organization competitive advantage (Hypotheses 7).

Table 5.39 Frequency competitive advantage question # 10: IT respondents

Competitive Advantage Question # 10

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	12	46.2	54.5	54.5
	agree	7	26.9	31.8	86.4
	strongly agree	3	11.5	13.6	100.0
	Total	22	84.6	100.0	
Missing	System	4	15.4		
Total		26	100.0		

In question 10, IT people responded in section 2 of questionnaire was about their company document exchange online tools enable companies to easily and safely exchange important even confidential information over the Internet. With their document exchange customers can comfortably send and receive critical business documents and other information forms like video, audio and text via the Internet and have full control over their digitally delivered documents. The question focused on “Customized reports about their customers and products”. In table 5.39, the frequency column reported that 7 of IT respondent came from “agree” and it was equivalent to 26.9 percent There were 3 of them chose “strongly agree” and it was equivalent to 7.7 %. Both 7 (agree) and 3 (strongly agree) of IT respondent believed and supported question on “Customized reports about their customers and products”. Other 12 of IT respondent did “not sure” about this question. In summary, there were significantly “strongly agree” and “agree” more than disagree which this question could sustain MIS security can significantly predict organization competitive advantage (Hypotheses 7).

In question 11, IT people responded in section 2 of questionnaire was about their company document exchange online tools enable companies to easily and safely exchange important even confidential information over the Internet. With their document exchange customers can comfortably send and receive critical business documents and other information forms like video, audio and text via the Internet and have full control

Table 5.40 Frequency competitive advantage question # 11: IT respondents

Competitive Advantage Question # 11

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	5	19.2	22.7	22.7
	agree	12	46.2	54.5	77.3
	strongly agree	5	19.2	22.7	100.0
	Total	22	84.6	100.0	
Missing	System	4	15.4		
Total		26	100.0		

over the digitally delivered documents. The question focused on "Improved accuracy; elimination of illegible handwritten records". In table 5.40, the frequency column reported that 12 of IT respondent came from "agree" and it was equivalent to 46.2 percent There were 5 of them chose "strongly agree" and it was equivalent to 19.2 %. Both 12 (agree) and 5 (strongly agree) of IT respondent believed and supported question on "Improved accuracy; elimination of illegible handwritten records". Other 5 of IT respondent did "not sure" about "Improved accuracy; elimination of illegible handwritten records".

In summary, there were significantly "strongly agree" and "agree" more than disagree which this question could sustain MIS security can significantly predict organization competitive advantage (Hypotheses 7).

Table 5.41 Frequency competitive advantage question # 12: IT respondents

Competitive Advantage Question # 12

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	10	38.5	45.5	45.5
	agree	11	42.3	50.0	95.5
	strongly agree	1	3.8	4.5	100.0
	Total	22	84.6	100.0	
Missing	System	4	15.4		
Total		26	100.0		

In question 12, IT responded in section 3 of questionnaire on "Their organizations ability to develop and experiment with VPN, which enable business processing and performance to take advantage of VPN and trends". In table 5.41, the frequency column reported that 11 of IT respondent came from "agree" and it was equivalent to 42.3 percent. There was 1 of respondent came from "strongly agree". This responds of IT can be supported the hypothesis on "VPN usage has significant effect on business processing" because these 11 (agree) and 1 (strongly agree) of IT respondent believed that their organizations ability to develop and experiment with VPN, which enable business processing and performance to take advantage of VPN and trends. Other 10 of IT respondent did "not sure" if their organizations ability to develop and experiment with new technologies, which enable they to take advantage of emerging technologies and trends or not.

In this question, there was significantly "agree" more than "not sure" as Likert response scale which IT compensated concentration on their organizations ability to develop and experiment with VPN, which enable business processing and performance to take advantage of VPN and trends. The result from these IT respondents could provide evidence and sustain that VPN usage has a significantly effect on business competitive advantage (Hypotheses 2).

Table 5.42 Frequency competitive advantage question # 13: IT respondents

Competitive Advantage Question # 13

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	7	26.9	31.8	31.8
	agree	7	26.9	31.8	63.6
	strongly agree	8	30.8	36.4	100.0
	Total	22	84.6	100.0	
Missing	System	4	15.4		
Total		26	100.0		

In question 13, IT responded in section 3 of questionnaire on "Their organization's ability to share information throughout the organization through effective VPN and improve business competitive advantage on this VPN system". In table 5.42, the frequency column reported that 7 of IT respondent came from "agree" and it was equivalent to 26.9 %. There were 8 of them chose "strongly agree" and it was equivalent to 30.8 %. Both 7 (agree) and 8 (strongly agree) of IT respondent believed that their organization's ability to share information throughout the organization through effective VPN and communication platforms. Other 7 of

IT respondent did "not sure" if their organization's ability to share information throughout the organization through effective VPN and communication platforms.

In summary, there were significantly "strongly agree" and "agree" more than "not sure" as Likert response scale which IT compensated concentration on their organization's ability to share information throughout the organization through effective VPN and improve business competitive advantage on this VPN system. The result from these IT respondents could provide evidence and sustain that VPN usage has a significantly effect on business competitive advantage (Hypotheses 2).

Table 5.43 Frequency competitive advantage question # 14: IT respondents

Competitive Advantage Question # 14

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	7	26.9	31.8	31.8
	agree	8	30.8	36.4	68.2
	strongly agree	7	26.9	31.8	100.0
	Total	22	84.6	100.0	
Missing	System	4	15.4		
Total		26	100.0		

In question 14, IT people responded in section 3 of questionnaire on "The ability of their MIS department to understand and use VPN for security and protection". In table 5.43, the frequency column reported that 8 of IT respondent came from "agree" and it was equivalent to 30.8 percent There were 7 of them chose "strongly agree" and it was equivalent to 26.6 percent. This responds of IT can be supported the hypothesis on "VPN usage has significant effect on MIS protection" because both 8 (agree) and 7 (strongly agree) of IT respondent believed that the ability of their MIS department to understand and use VPN for security and protection. Other 4 of IT respondent did "not sure" about this question.

In summary, there were significantly "strongly agree" and "agree" more than "not sure" as Likert response scale which IT compensated concentration on the ability of their MIS department to understand and use VPN for security and protection. The result from these IT respondents could provide evidence and sustain that VPN usage has a significantly effect on MIS protection (Hypotheses 3).

Table 5.44 Frequency competitive advantage question # 15: IT respondents

Competitive Advantage Question # 15

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	10	38.5	45.5	45.5
	agree	8	30.8	36.4	81.8
	strongly agree	4	15.4	18.2	100.0
	Total	22	84.6	100.0	
Missing	System	4	15.4		
Total		26	100.0		

In question 15, IT responded in section 3 of questionnaire on "Their organizations ability to anticipate future changes and growth as perditions in VPN system capability, to choose information security technology that can accommodate this change and to efficiently mange the resulting technology change and growth". In table 5.44, the frequency column reported that 8 of IT respondent came from "agree" and it was equivalent to 30.8 percent. There were 4 of them chose "strongly agree" and it was equivalent to 15.4 percent. Both 8 (agree) and 4 (strongly agree) of IT respondent believed that their organizations ability to anticipate future changes and growth, to chose information security technology that can accommodate this change and to efficiently mange the resulting technology change and growth. Other 10 of IT respondent did "not sure" if their organizations ability to anticipate future changes and growth, to chose information security technology that can accommodate this change and to efficiently mange the resulting technology change and growth or not.

In summary, there were insignificantly "strongly agree" and "agree' more than "not sure" in Likert response scale which IT compensated concentration on their organizations ability to anticipate future changes and growth as perditions in VPN system capability, to choose information security technology that can accommodate this change and to efficiently mange the resulting technology change and growth. IT professional could distinguish the different after the implementation of VPN. The result from this question 15 could verify that the variation business objectives can significantly predict system capability (Hypotheses 6) such as implementation of VPN.

Table 5.45 Frequency competitive advantage question # 16: IT respondents

Competitive Advantage Question # 16

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	3	11.5	13.6	13.6
	agree	7	26.9	31.8	45.5
	strongly agree	12	46.2	54.5	100.0
	Total	22	84.6	100.0	
Missing	System	4	15.4		
Total		26	100.0		

In question 16, IT people responded in section 3 of questionnaire on "Their organization's IT ability to ensure business performance and IS strategies are integrated with organizational functional plans and IS align with organizational needs".In table 5.45, the frequency column reported that 7 of IT respondent came from "agree" and it was equivalent to 26.9 percent. There were 12 of them chose "strongly agree" and it was equivalent to 46.2 percent. This responds of IT can be supported the hypothesis on "IT objective can significantly improve business performance" because both 7 (agree) and 12 (strongly agree) of IT respondent believed that their organization's IT ability to ensure business performance and IS strategies are integrated with organizational functional plans and IS align with organizational needs. There were 3 of IT respondent did "not sure" if their organization's IT ability to ensure business performance and IS strategies are integrated with organizational functional plans and IS align with organizational needs.

Table 5.46 Frequency competitive advantage question # 17: IT respondents

Competitive Advantage Question # 17

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	1	3.8	4.5	4.5
	agree	7	26.9	31.8	36.4
	strongly agree	14	53.8	63.6	100.0
	Total	22	84.6	100.0	
Missing	System	4	15.4		
Total		26	100.0		

In question 17, IT responded in section 3 of questionnaire on "Their MIS security ability to gain competitive advantage and secure information system in organization". In table 5.46, the

frequency column reported that 7 of IT respondent came from "agree" and it was equivalent to 26.9 percent. There were 14 of them chose "strongly agree" and it was equivalent to 53.8 %. This responds of IT can be supported the hypothesis on "MIS security can significantly predict organizational competitive advantage" because both of 7 (agree) and 14 (strongly agree) of IT respondent believed that their MIS security ability to gain competitive advantage and secure information system in organization. There was only 1 of IT respondent came from "not sure" if their MIS security ability to gain competitive advantage and secure information system in organization or not.

In summary, there were insignificantly "strongly agree" and "agree' more than "not sure" in Likert response scale which IT compensated concentration on their MIS security ability to gain competitive advantage and secure information system in organization. IT professional could distinguish the different after the implementation of VPN. The result from this question 17 could verify that MIS security can significantly predict organisational competitive advantage (Hypotheses 7).

5.1.7.3 Summary

In summary of phase two clarified and uncovered on information security and competitive advantage which used descriptive statistics to present quantitative descriptions in a manageable form. Descriptive statistics help this study to simplify large amounts of data in a sensible way. Each descriptive statistic reduces lots of data into a simpler summary. Although both the mean and median of the performance measures are reported for both samples, the medians are considered to be better indicators. As above sections and tables discussed and explained details of each questionnaire which had responded by business and IT professional. In this way, research could find out on information security technology and competitive advantage as research questions and testing the hypothesis. Data of phase two can be used and analysis in more details in correlation and regression in section 3 research analyses as triangulation of data.

5.1.8 Phase Three of Data Analysis

In this section, there were 7 observation questions which had used for VPN users at their work places. Researcher had met each of VPN users and asked each user to fill up the VPN user observation survey. In this visiting, research was able to watched VPN users how they used VPN system. Some of VPN users were worked in MIS and information system (IS) department. Research interviewed business and IT professional on VPN system by meeting in each business and IT at their working place (see section 2.8.2).

5.1.8.1 Research Findings

In this phase, descriptive statistics were used to describe the basic features of VPN user observation. They provide simple summaries about the sample and the measures of this observation as interpretive in triangulation method. Together with simple analysis, they form the basis of virtually every quantitative analysis of data. With descriptive statistics author could simply describing what was or what the data shows. Descriptive Statistics were used to present quantitative descriptions in a manageable form. Descriptive statistics help this study to simply large amounts of data in a sensible way. Each descriptive statistic reduces lots of data into a simpler summary.

5.1.8.2 Business and IT Findings

The results for VPN observation in questions 1 -7 are displayed in Table 5.47 (median, mean, and standard deviation). Although both the mean and median of the performance measures are reported for both samples, the medians are considered to be better indicators. The Means procedure calculates subgroup means and related univariate statistics for dependent variables within categories of one or more independent variables. Across all rows of the table 5.47, the mean column shows how average questionnaire differs by VPN users within level of sections. The standard deviation is a measure of how widely values are dispersed from the average value (the mean). In this observation one was look into "user configures connections to a VPN server, start connections, enrol for certificates to authenticate connections to VPN servers, and display events from the log".

In table 5.48, the frequency column reported that 21 of VPN user came from "agree". This was equivalent to 80.8 percent of total number of VPN users.

Table 5.47 Observation VPN User: Mean, Median, and Standard Deviation

Observation/ Question	Mean	Media	STDEV
1. Lets you configure connections to a VPN server, start connections, enrol for certificates to authenticate connections to VPN servers, and display events from the log.	3.92	3	0.400
2. Lets you manually change the size	3.88	3	0.440

of the maximum transmission unit.			
3. Making sure users are who they say they are, by usernames, group names and passwords.	4.12	3	.440
4. Establishing user access rights—Hours of access, connection time, and allowed destinations, allowed protocols, and so on.	4.20	.577	3
5. Managing security keys for encryption and decryption. Authenticating, encrypting, and decrypting data through the tunnel.	4.12	.526	3
6. Lets you safely remove the VPN Client software from your system and retain your connection and certificate configurations.	4.28	.458	4
7. You can transmit sensitive information over the Internet without needing to worry about who might see.	4.12	6.00	3

Table 5.48 Frequency on Observation VPN User # 1

VPN Observation # 1

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	3	11.5	12.0	12.0
	agree	21	80.8	84.0	96.0
	strongly agree	1	3.8	4.0	100.0
	Total	25	96.2	100.0	
Missing	System	1	3.8		
Total		26	100.0		

There was 1 of them chose "strongly agree" or equivalent to 3.8 percent. Both 21 (agree) and 1 (strongly agree) of VPN users believed that they could configures connections to a VPN server, start connections, enrol for certificates to authenticate connections to VPN servers, and display events from the log. Other 3 of respondents did "not sure" if they could connections to a VPN server, start connections, enrol for certificates to authenticate connections to VPN servers, and display events from the log.

In summary, there was significantly strongly agree and agree more than disagree which this question could sustain MIS security can significantly predict organization competitive advantage (Hypotheses 7).

Table 5.49 Frequency on Observation VPN User # 2

VPN Observation Question # 2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	4	15.4	16.0	16.0
	agree	20	76.9	80.0	96.0
	strongly agree	1	3.8	4.0	100.0
	Total	25	96.2	100.0	
Missing	System	1	3.8		
Total		26	100.0		

In this observation was look into "if user can manually change the size of the maximum transmission unit." In table 5.49, the frequency column reported that 20 of VPN user came from "agree". This was equivalent to 76.9 % of total number of VPN users. There was 1 of them chose "strongly agree" or equivalent to 3.8. Both 20 (agree) and 1 (strongly agree) of VPN users said that they could manually change the size of the maximum transmission unit.

Other 4 of respondents did "not sure" if they could manually change the size of the maximum transmission unit. In summary, there were significantly "strongly agree" and "agree" more than "not sure" as Likert response scale which VPN user compensated concentration on if user can manually change the size of the maximum transmission unit. The result from these business respondents could provide evidence and sustain that VPN usage has a significantly effect on MIS protection (Hypotheses 3).

Table 5.50 Frequency on Observation VPN User # 3

VPN Observation Question # 3

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	1	3.8	4.0	4.0
	agree	20	76.9	80.0	84.0
	strongly agree	4	15.4	16.0	100.0
	Total	25	96.2	100.0	
Missing	System	1	3.8		
Total		26	100.0		

In this observation was look into "user authentication: Making sure users are who they say they are, by usernames, group names and passwords." In table 5.50, the frequency column reported that 20 of VPN user came from "agree". This was equivalent to 76.9 % of total number of VPN users. There were 4 of them chose "strongly agree" or equivalent to 15.4 %. There were 24 of VPN users said that they agreed (20) and strongly agreed (4) on "user authentication: Making sure users are who they say they are, by usernames, group names and passwords". There was only one did "not sure" on this question.

In summary, there was significantly strongly agree and agree more than disagree which this question could sustain MIS security can significantly predict organization competitive advantage (Hypotheses 7).

Table 5.51 Frequency on Observation VPN User # 4

VPN Observation Question # 4

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	2	7.7	8.0	8.0
	agree	16	61.5	64.0	72.0
	strongly agree	7	26.9	28.0	100.0
	Total	25	96.2	100.0	
Missing	System	1	3.8		

Total	26	100.0		

This observation was look into "Establishing user access rights: Hours of access, connection time, and allowed destinations, allowed protocols, and so on." In table 5.51, the frequency column reported that 16 of VPN user came from "agree". This was equivalent to 61.5 % of total number of VPN users. There were 7 of them chose "strongly agree" or equivalent to 26.9 %. There were 23 of VPN users said that they agreed (20) and strongly agreed (4) on "Establishing user access rights: Hours of access, connection time, and allowed destinations, allowed protocols, and so on." Other 2 of VPN users did "not sure" on establishing user access rights: Hours of access, connection time, and allowed destinations, allowed protocols, and so on. In summary, there was significantly strongly agree and agree more than disagree which this question could sustain MIS security can significantly predict organization competitive advantage (Hypotheses 7).

Table 5.52 Frequency on Observation VPN User # 5

VPN Observation Question # 5

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	2	7.7	8.0	8.0
	agree	18	69.2	72.0	80.0
	strongly agree	5	19.2	20.0	100.0
	Total	25	96.2	100.0	
Missing	System	1	3.8		
Total		26	100.0		

This observation was look into "Managing security keys for encryption and decryption for example, authenticating, encrypting, and decrypting data through the tunnel." In table 5.52, the frequency column reported that 18 of VPN user came from "agree". This was equivalent to 69.2 % of total number of VPN users. There were 5 of them chose "strongly agree" or equivalent to 19.2 %. There were 23 of VPN users said that they agreed (18) and strongly agreed (5) on "Managing security keys for encryption and decryption for example, authenticating, encrypting, and decrypting data through the tunnel." Other 2 of VPN user respondent came from "not sure" about "Managing security keys for encryption and decryption for example, authenticating, encrypting, and decrypting data through the tunnel." In summary, there was significantly strongly agree and agree more than disagree which this

question could sustain MIS security can significantly predict organization competitive advantage (Hypotheses 7).

The observation was look into "if user safely removes the VPN Client software from his or her system and retains his or her connection and certificate configurations." In table 5.53, the frequency column reported that 18 of VPN user respondent came from "agree". This was equivalent to 69.2 % of total number of VPN users. There were 7 of them chose "strongly agree" or equivalent to 26.9 %.

Table 5.53 Frequency on Observation VPN User # 6

VPN Observation Question # 6

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	agree	18	69.2	72.0	72.0
	strongly agree	7	26.9	28.0	100.0
	Total	25	96.2	100.0	
Missing	System	1	3.8		
Total		26	100.0		

There were 25 of VPN users said that they agreed (18) and strongly agreed (7) on "if user safely removes the VPN Client software from his or her system and retains his or her connection and certificate configurations." In summary, there was significantly strongly agree and agree more than disagree which this question could sustain MIS security can significantly predict organization competitive advantage (Hypotheses 7).

Table 5.54 Frequency on Observation VPN User # 7

VPN Observation Question # 7

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not sure	3	11.5	12.0	12.0
	agree	16	61.5	64.0	76.0
	strongly agree	6	23.1	24.0	100.0
	Total	25	96.2	100.0	
Missing	System	1	3.8		
Total		26	100.0		

This observation was look into "if user can transmit sensitive information over the Internet without needing to worry about who might see it." In table 5.54, the frequency column

reported that 16 of VPN user came from “agree”. This was equivalent to 61.5 % of total number of VPN users. There were 6 of them chose “strongly agree” or equivalent to 23.1 %. There were 22 of VPN users said that they agreed (16) and strongly agreed (6) and believed that if they can transmit sensitive information over the Internet without needing to worry about who might see it. There 3 of VPN user respondent did “not sure” if they can transmit sensitive information over the Internet without needing to worry about who might see it.

In summary, there was significantly strongly agree and agree more than disagree which this question could sustain MIS security can significantly predict organization competitive advantage (Hypotheses 7).

In the following interview, the researcher asked the VPN user at work place for some additional information concerning VPN security technology, especially with regard to the business and IT professional.

[Researcher] What does VPN can help and sustain you for work as user’s perspective?

[Marketing Manager] Yes, I’m as user. I can bring work at home or on the road which allows me to use VPN connections to establish a remote access connection to my firm’s server by using the infrastructure provided by a public network such as the Internet. I use VPN to connect point-to-point connection between my desktop (the VPN client) and an organization server (the VPN server). The exact infrastructure of the shared or public network is irrelevant because it appears logically as if the data is sent over a dedicated private link.

[Researcher] Can your firm get benefit of VPN?

[Marketing Manager] Yes, our organizations can also use VPN connections to establish router-to-router connections with geographically branch offices or with suppliers over a public network such as the Internet while maintaining secure communications. We very much feel secure during our business process.

[Researcher] What is the strategic role of security in the firm?

[IT Manager] There are risks to investing in security to the extent that investment includes information sharing. The risk of possible losses in consumer trust and reputation discourages firms from sharing security information. Yet further we has verified that information sharing is both economically valuable and a complement to security investment. We think information sharing has shown that information sharing is most valuable in highly competitive markets, because it counters downward pressures on pricing.

[Researcher] What is the role of individual incentives on privacy and security?

[IT Manager] IT manager explained that the previous work assumes that privacy is good for individuals and good in some cases for firms. Yet, the information market is not always a

zero-sum game in which gains from the consumer are offset by loses for the firm. Sharing information that is good for one party may not be in the interest of the other party. Privacy can be good for individuals or bad, e.g., when the information obtained by others is used to lower prices or to extend privileges. In particular, the opposite of privacy in the market is not necessarily information; the opposite of privacy is price discrimination. In markets where there is zero marginal cost (e.g., information markets) firms must be able to extract consumer surplus by price discrimination. This means that our firms cannot charge what we pay, at the margin, but must charge what the consumer is willing to pay. Data the consumer considers to be privacy violations may be necessary pricing data to the merchant.

Individual rejection of security information may itself be rational. When information security means ensuring that the end user has no place to hide his or her own information, or when security is implemented to exert detailed control over employees, individuals rightly seek to subvert the control. Security is often built with perverse incentives. Privacy and security are constructed to be opposites instead of complements in controlling information. Rejection of security is, in some cases, strictly rational.

[Researcher] Have you seen or noticed weak point of VPN?

[Senior system engineer] The weak point in the fence is obvious for companies that use remote-access virtual private network (VPN) systems to allow out-of-office use of corporate resources. Many remotely connected clients don't have systems patched and assessed as rigorously as those that are permanent parts of the enterprise network. Furthermore, when performing security assessments for customers, we always find exceptions to security policies and technology limitations to client management.

[Researcher] How do you support and help user to solve problem of using system?

[Senior system engineer] User and support notification: When a client computer fails the evaluation process, the user should be notified of the problem in a very detailed manner, and his next step should be clearly defined. Automatic notification of support teams or a network operations center is a valuable complementary feature, as the quarantine failure may signal a compromised asset or user in need of assistance. Right now, most quarantine systems address remote-user VPN scenarios but don't support other modes of access such as LANs. Nevertheless, Cisco Systems Inc., which introduced a quarantine product last fall, plans to extend its functionality throughout a Cisco-based network.

[Research] Could describe strong authentication of User and Devices at your organization?

[MIS Manager] We have VPN solution enables strong authentication of users and devices via digital certificates to help provide protection from hackers or attempts to impersonate

legitimate users, as intruders need to have access to a user's digital certificate along with the code to unlock it. This solution offers flexibility in how digital certificates are stored and used. Digital certificates can be stored encrypted on the user's computer, smart card, USB token or made available through a secure credential server

[Researcher] Could you give me more details on digital certificate?

[MIS Manager] Digital certificates are easy for administrators to deploy and manage. We use VPN technology, the entire enrollment, authentication and installation process for digital certificates is built to be accomplished in a single operation without manual intervention by an administrator. This automated feature enables rapid scalability suitable for large user environments. From an end-user's perspective, strongly authenticating themselves with digital certificates is virtually transparent

[Researcher] How about the cost-effective of VPN technology?

[MIS manager] We believe VPN technology offers a cost-effective, strong authentication solution for securing our organization's VPN. Though user name and password authentication is thought to be an easy-to-manage and cost-effective approach to securing a VPN, in reality password management issues and help desk calls related to passwords quickly lead to escalating hidden costs for organizations using VPN.

[Researcher] Do you often change your security policy?

[MIS manager] We found out that security threats change quickly. Therefore, our definition of policy should be extremely flexible. This is often accomplished through scripting for our staff actions. However, not all rules should require extensive scripting. Client response should be fast, and evaluation of common settings such as routing table, file integrity and software existence should be performed quickly.

[Researcher] Do you think enterprises have really accepted that poor data quality is a widespread problem? How do you overcome the inertia of corporate culture when it comes to making the changes necessary to establish enterprise security system?

[Product Manager] I have seen some important changes in management attitudes towards data quality over the past ten years. During the mid-1990s, it would not be unusual for a level manager to pay lip service to data quality as a key enterprise requirement, but the levels of investment in information quality improvement were limited in both scope and vision, typically depending on the use of a commercial-off-the-shelf software data quality package managed by a single Information Technology (IT) staff member.

[Researcher] Do you think the makers of most large enterprise security systems have taken the time necessary to ensure that good quality data is collected by your software? Where has your organization failed?

[Product manager] our people have a natural tendency to believe in the soundness of the processes in which our system and security product are being used, and so it would not surprise me that many application systems take the quality of the information used within for granted. On the other hand, the individuals using these security systems must be able to get their jobs done, even when the application does not appropriately support all potential operational use cases. The upshot is that clever people will always find a way to get that data into the system, and this is often how invalid or inappropriate data is introduced into a system.

[Researcher] What do you think about your organization and competitive advantage? You think your firm gains competitive advantage.

[Produce Manager] I do have hope that as approaches that companies like ours have taken in helping our clients value information as an organizational asset will encourage a closer inspection of the short and long-term return on investment in data quality improvement. Those companies that see that their data used to run the business can also be used to improve their business will see that measurably high-quality information provides significant competitive advantage.

[Researcher] Could you describe your organization's VPN? How VPN can facilitate your organization?

[Managing Director] A VPN enables our business to securely connect remote users, branch offices, business partners, and customers using encrypted connections over a public network such as the internet. Our companies can use VPNs to gain an advantage in such a highly competitive and regulated industry.

[Researcher] Do you have good experience of using VPN in your organization?

[Managing Director] We have increased speed and much more flexibility. VPN operate independent of the underlying telecommunications infrastructure. As a result, it can be deployed quickly using any internet connection. A collaborative investigation between our company and partner can be established in minutes and maintained for months. New acquisitions can be brought online by using the VPN as either a temporary or permanent solution.

[Researcher] Do you think your security has improved and more effective?

[Managing Director] We found and noticed that VPN guarantee the identity of individuals

and systems, ensure the privacy and integrity of transmitted information, and limit the access of each participant to the resources that are authorized for use. Rather than build security into each application and service individually, VPNs build security into the communications infrastructure only once for all applications. External and internal communications also benefit from this security implementation.

5.1.8.3 Summary

In summary of last phase, there was useful information which had corrected during VPN observation. Researcher could watch VPN users whom interacted with VPN system and found out that they were very positive and confidence in using VPN at work. There was tremendously additional information during interviewing with business and IT professional.

5.2 RESEARCH ANALYSIS

Researcher used both correlation and regression for data analysis including correlation matrix, correlation significant at the 0.05 level (2-tailed), R^2, and F-statistic. In this study, business and IT are two different sets of data which need to measurement scales. The measurement scales used should be at least interval scales, but other correlation coefficients are available to handle other types of data. Correlation coefficients can range from -1.00 to +1.00. The value of -1.00 represents a perfect negative correlation while a value of +1.00 represents a perfect positive correlation. The significance level calculated for each correlation is a primary source of information about the reliability of the correlation. The test of significance is based on the assumption that the distribution of the residual values (i.e., the deviations from the regression line) for the dependent variable y (questionnaire) follows the normal distribution, and that the variability of the residual values is the same for all values of the independent variable x (Business or IT).

Regression analysis is a tool used by economists and others to estimate the relationships among a dependent variable Y and one (or many) independent variable(s) X. The purpose of regression analysis is the best fit data points from a straight line down on an XY graph. This analysis and model can determine the effect that an intervention has on organizational performance and business processing after statistically controlling for the effects of other factors that can also affect performance and processing. In next two sections illustrate in measurement validation and the triangulation of data including correlation matrix, R^2, and F-statistic.

5.2.1 Measurement Validation

To begin the analysis, consider the correlations in Tables (5.55 – 5.58) as below. This type of table is called a correlation matrix. It lists the variable names in each phase and questionnaire down the first column and across the first row (see tables 5.55 – 5.58). The diagonal of a correlation matrix (i.e., the numbers that go from the upper left corner to the lower right) always consists of ones. That's because these are the correlations between each variable and itself (and a variable is always perfectly correlated with itself). The result only shows the lower triangle of the correlation matrix. In every correlation matrix there are two triangles that are the values below and to the left of the diagonal (lower triangle) and above and to the right of the diagonal (upper triangle). There is no reason to illustrate both triangles because the two triangles of a correlation matrix are always mirror images of each other (the correlation of variable x with variable y is always equal to the correlation of variable y with variable x). When a matrix has this mirror-image quality above and below the diagonal we refer to it as a symmetric matrix. A correlation matrix is always a symmetric matrix.

The relationship between two sets (business and IT) of data, that when one changes, the other is likely to make a corresponding change. If the changes are in the same direction, then there is a "positive" correlation. If it is in the opposite direction, then it is a "negative" correlation. To locate the correlation for any pair of variables, find the value in the table for the row and column intersection for those two variables. From tables 5.55 to 5.58 use Correlation significant at the 0.05 level (2-tailed) with * and ** for Correlation significant at the 0.01 level (2-tailed). For example, to find the correlation matrix in table 5.54 between variables "Operational Cost" at row IPSEC 3 and "Remote Access" at column IPSEC1. The result of correlation is -.064 which has no relationship between operational cost and remote access.

Tables 5.55 to 5.58 represents two sets of variables between business and IT professional and F-statistic as regression model. As predictors are added to the model, each predictor can explain some of the variance in the dependent variable simply due to chance. One could continue to add predictors to the model which would continue to improve the ability of the predictors to explain the dependent variable, although some of this increase in R-square would be simply due to chance variation in that particular sample. The adjusted R-square attempts to yield a more honest value to estimate the R-squared for the population. F and Sig. - The F-value is the Mean Square Regression divided by the Mean Square Residual, yielding F. The p-value associated with this F value is very small (0.0000). These values are

used to answer the question the independent (Business or IT professional) variables reliably predict the dependent variable.

Table 5.55 Phase One VPN Business Respondent: Correlation Matrix

VPN Protocol		IPSEC1	L2TP1	PPTP1	IPSEC2	L2TP2	PPTP2	IPSEC3	L2TP3	PPTP3	IPSEC4	L2TP4	PPTP4	IPSEC5	L2TP5	PPTP5	IPSEC6	L2TP6	PPTP6
Remote Access	IPSEC1	1.000																	
	L2TP2	-.199	1.000																
	PPTP3	-.267	.403	1.000															
Tunnel & Authenticate	IPSEC2	.466*	-.173	-.115	1.000														
	L2TP2	-.022	.221	-.175	-.338	1.000													
	PPTP2	-.156	.380	.515*	-.257	.130	1.000												
Operational Cost	IPSEC3	-.064	-.051	.123	.013	-.301	.084	1.000											
	L2TP3	-.316	.204	-.078	-.372	.079	.089	.155	1.000										
	PPTP3	.067	.320	.312	.273	-.200	.316	.439*	-.062	1.000									
Quality of Service	IPSEC4	-.243	.341	.285	-.147	.370	.401	-.101	-.248	-.031	1.000								
	L2TP4	-.216	.172	-.131	-.249	-.111	-.344	-.045	.255	-.002	-.255	1.000							
	PPTP4	.010	-.092	-.181	-.100	.163	.001	-.066	.184	.198	-.215	.140	1.000						
Scalability	IPSEC5	.121	.324	.399	.061	.096	.119	.051	-.121	.439*	.217	.165	.193	1.000					
	L2TP5	-.247	.216	.005	-.268	.381	-.012	-.104	.204	-.271	.414*	-.311	.085	-.041	1.000				
	PPTP5	-.411*	-.041	.056	-.427*	.287	.015	-.051	.058	-.160	.221	-.352	.020	-.153	.469*	1.000			
LAN Access	IPSEC6	-.325	-.038	.078	-.211	.178	.370	-.306	.037	-.290	.215	-.484*	.086	-.364	.248	.597*	1.000		
	L2TP6	.165	-.002	-.156	.005	-.234	-.150	.097	-.071	.105	.105	.181	.058	.016	.071	-.265	-.268	1.000	
	PPTP6	.198	-.109	-.184	.322	-.449*	-.381	-.169	.023	-.051	-.521**	.104	.266	-.060	.027	-.342	-.180	.293	1.000
N		24	24	24	24	24	24	24	24	24	24	24	24	24	24	24	24	24	24

* Correlation is significant at the 0.05 level (2-tailed).
** Correlation is significant at the 0.01 level (2-tailed).

Table 5.56 Phase One VPN IT Respondent: Correlation Matrix

VPN Protocol		IPSEC1	L2TP1	PPTP1	IPSEC2	L2TP2	PPTP2	IPSEC3	L2TP3	PPTP3	IPSEC4	L2TP4	PPTP4	IPSEC5	L2TP5	PPTP5	IPSEC6	L2TP6	PPTP6
Remote Access	IPSEC1	1.000																	
	L2TP1	-.345	1.000																
	PPTP1	-.253	.311	1.000															
Tunnel & Authenticate	IPSEC2	.025	-.284	.020	1.000														
	L2TP2	.296	.206	.157	-.285	1.000													
	PPTP2	.129	.008	.249	-.352	.513*	1.000												
Operational Cost	IPSEC3	.270	.101	.346	.029	.452*	.552*	1.000											
	L2TP3	.346	-.297	-.006	-.138	.277	-.287	-.141	1.000										
	PPTP3	.182	-.367	-.155	-.497*	-.025	-.003	-.263	.477*	1.000									
Quality of Service	IPSEC4	-.005	-.006	.050	-.222	.050	-.078	.035	.157	.113	1.000								
	L2TP4	.190	-.473*	-.182	-.065	-.230	.015	-.482*	.186	.360	-.219	1.000							
	PPTP4	.095	-.129	.134	-.093	.101	.312	.222	-.063	.335	-.218	.128	1.000						
Scalability	IPSEC5	-.207	.032	.149	-.354	-.204	.170	-.002	.084	.167	-.163	.321	-.032	1.000					
	L2TP5	.193	-.472*	-.185	-.061	-.229	.011	-.485*	.185	.355	-.213	1.000**	.126	.315	1.000				
	PPTP5	.038	.018	.224	.054	.072	.185	.197	-.082	.171	-.251	-.016	.905**	-.089	-.017	1.000			

LAN Access	IPSEC6	.125	-.364	-.051	-.280	-.137	.036	-.406	.143	.575**	-.205	.466**	.437*	-.070	.462*	.328	1.000		
	L2TP6	.149	.202	.179	.116	.036	-.146	-.078	.050	-.227	-.305	.139	-.286	-.045	.145	-.367	-.167	1.000	
	PPTP6	-.391	.026	.390	.176	-.062	-.046	-.062	.113	-.281	.065	-.151	-.301	-.145	-.155	-.253	-.137	.172	1.000
	N	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21

* Correlation is significant at the 0.05 level (2-tailed).

** Correlation is significant at the 0.01 level (2-tailed).

Table 5.57 Phase Two Competitive Advantage Business Respondent: Correlation Matrix

Competitive Advantage	Q 1	Q 2	Q 3	Q 4	Q 5	Q 6	Q 7	Q 8	Q 9	Q 10	Q 11	Q 12	Q 13	Q 14	Q 15	Q 16	Q 17
Question # 1	1.000																
Question # 2	-.670**	1.000															
Question # 3	.332	-.133	1.000														
Question # 4	-.171	.255	.082	1.000													
Question # 5	.151	-.131	.191	-.033	1.000												
Question # 6	-.120	.073	-.572**	-.008	-.079	1.000											
Question # 7	-.013	-.066	-.051	.070	.300	-.142	1.000										
Question # 8	-.143	.103	-.322	.422**	-.289	.329	-.253	1.000									
Question # 9	-.265	.115	.041	-.304	.027	.407*	-.451*	.077	1.000								
Question # 10	-.113	.078	-.342	-.237	-.083	.102	-.062	.027	.030	1.000							
Question # 11	-.389*	.230	.133	.103	-.247	-.285	-.447*	.009	.165	-.078	1.000						
Question # 12	.195	-.047	.248	-.541**	-.146	-.249	-.087	-.529**	-.095	.020	.291	1.000					
Question # 13	.012	.140	.292	.177	.062	-.154	.151	-.065	-.087	.057	.256	.300	1.000				
Question # 14	-.179	.113	-.292	-.149	.086	.022	.119	.177	-.035	.373	.042	.112	.239	1.000			
Question # 15	.184	-.052	.172	-.146	.135	-.345	.100	-.232	-.287	.161	.126	.589*	.309	.116	1.000		
Question # 16	-.283	.219	-.251	.056	-.345	-.113	-.328	.228	-.142	.164	.392*	.120	.120	.124	.166	1.000	
Question # 17	.246	.152	.305	.594	-.051	-.096	.008	.172	-.323	-.258	-.255	-.211	-.007	-.352	.068	.046	1.000
Adjusted R^2	-.037	-.019	-.002	-.009	-.042	-.031	-.041	-.036	-.042	-.030	-.011	-.041	-.006	-.034	-.041	.093	-.035
F	.110	.532	.962	.783	.000	.256	.017	.130	.000	.268.	.719	.006	.850	.176	2.081	3.564	.164
Significant	.743[a]	.473[a]	.337[a]	.385[a]	.984[a]	.618[a]	.898[a]	.721[a]	.984[a]	.609[a]	.405[a]	.938[a]	.366[a]	.678[a]	.162[a]	.071[a]	.689[a]
N	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26

** Correlation is significant at the 0.01 level (2-tailed).
* Correlation is significant at the 0.05 level (2-tailed).

Table 5.58 Phase Two Competitive Advantage IT Respondent: Correlation Matrix

Competitive Advantage	Q 1	Q 2	Q 3	Q 4	Q 5	Q 6	Q 7	Q 8	Q 9	Q 10	Q 11	Q 12	Q 13	Q 14	Q 15	Q 16	Q 17
Question # 1	1.000																
Question # 2	-.262	1.000															
Question # 3	.059	-.016	1.000														
Question # 4	.204	.212	.107	1.000													
Question # 5	.007	-.205	.330	-.027	1.000												
Question # 6	.219	.069	.023	.270	-.144	1.000											
Question # 7	-.131	-.054	-.018	-.148	.044	-.066	1.000										
Question # 8	-.114	-.048	-.130	.098	.039	-.058	-.054	1.000									
Question # 9	-.338	.211	-.011	-.250	-.058	.313	-.177	-.155	1.000								
Question #10	-.191	.212	-.311	.069	.267	.010	.020	.309	-.055	1.000							
Question # 11	-.204	.130	.005	.005	-.092	-.270	-.112	.016	.130	.026	1.000						
Question # 12	-.332	.137	.242	-.498*	-.129	-.254	-.016	-.014	.043	-.023	.202	1.000					
Question # 13	-.182	.280	.016	.130	.205	-.196	.187	.048	-.089	.176	.441*	.165	1.000				
Question # 14	.103	-.062	-.089	-.191	.184	.166	.528	.043	.030	.246	-.014	.149	.376	1.000			
Question # 15	-.311	-.006	.169	-.088	-.193	-.324	-.007	.125	-.187	.209	-.041	.433*	-.256	-.113	1.000		
Question # 16	-.430	.281	-.197	.051	.006	-.361	.177	.281	-.024	.153	.320	.209	.602**	.201	.019	1.000	
Question # 17	.266	-.025	.434*	.434*	.334	.575**	-.028	-.025	-.064	.072	-.301	-.319	-.246	-.100	-.291	-.360	1.000
Adjusted R^2	-.025	.114	.108	-.044	-.048	-.042	-.026	-.035	-.046	-.028	-.040	-.031	-.047	-.042	-.018	-.025	-.043
F	.479	3.710	3.532	.107	.035	.153	.464	.294	.072	.420	.184	.366	.053	.155	.627	.494	.129
Significant	.497[a]	.068[a]	.075[a]	.747[a]	.853[a]	.700[a]	.504[a]	.594[a]	.791[a]	.524[a]	.673[a]	.552[a]	.820[a]	.698[a]	.438[a]	.490[a]	.724[a]
N	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22

* Correlation is significant at the 0.05 level (2-tailed).
** Correlation is significant at the 0.01 level (2-tailed).

Table 5.59 Phase Three VPN Observation: Correlation Matrix

VPN Observation	Q1	Q 2	Q 3	Q 4	Q 5	Q 6	Q 7
Question # 1	1.000						
Question # 2	-.057	1.000					
Question # 3	-.180	.293	1.000				
Question # 4	-.289	-.230	-.427*	1.000			
Question # 5	-.151	-.476*	-.065	.055	1.000		
Question # 6	-.100	-.240	.240	.094	-.145	1.000	
Question # 7	.215	.057	-.057	.048	-.312	.024	1.000
Adjusted R^2	.067	-.042	-.026	-.029	-.034	-.033	.035
F	2.726	.034	.388	.323	.218	.227	1.862
Significant	.112[a]	.855[a]	.540[a]	.575[a]	-.645[a]	.638[a]	.186[a]
N	25	25	25	25	25	25	25

* Correlation is significant at the 0.05 level (2-tailed).

5.2.2 Hypotheses Testing

This section presents the measurement properties, and results of hypothesis testing. Hypotheses postulating direct effects between constructs from H1 to H7 were tested based on questionnaires in three different phases. The mediation hypotheses were tested from phases one to three.

Table 5.60 Hypotheses Testing

Hypotheses	Support	Evidence
H1: There is no significant difference between IT and business objectives.	No	Documented in sub section 5.1.6
H2: Business objective bias can significantly predict systems capability.	Yes	Documented in sub section 5.1.6
H3: IT objective bias can significantly predict systems capability.	Yes	Documented in sub section 5.1.6
H4: VPN usage has a significant effect on MIS protection.	Yes	Documented in sub section 5.1.7
H5: VPN usage has a significant effect on business competitive advantage.	Yes	Documented in sub section 5.1.7
H6: The variation between IT/Business objectives can significantly predict systems capability.	Yes	Documented in sub section 5.1.7
H7: MIS security can significantly predict organizational competitive advantage.	Yes	Documented in sub section 5.1.8

Hypothesis 1, Not Supported: These results of AHP ratio-scale between Business and IT could notify the significant difference between business and IT objective. In phase one, business and IT professional could make judgments about the importance of lower level objectives or alternatives where they have the knowledge of the subject matter (see sub sub-section 5.1.6.2). This category refers to the understanding by IT professionals of the specific organizational context in which information security technology is deployed and of the connections between IT and the business. This knowledge enables IT professionals to see the big picture of IT in their current organization, to make linkages between different organizational units, and ensures focus on a larger perspective needed to benefit from the potential fit between the IT and the organizational context. It represents a holistic view of the organization and its current activities. This knowledge represents the capability for business understanding of IT professionals.

Hypothesis 2, Supported: AHP ratio-scale could illustrate business objective bias can significantly predict systems capability such as VPN security technology. The study provided

evidence in support of the existence and performance effects of using VPN as information security technology.

Hypothesis 3, Supported: The outcome of the analysis could advise IT objective can significantly improved business performance by using VPN system in their organizations. In a business environment where IT is used to gain business value, IT professionals must have an understanding of what their organization is about, that is, the business context in which information security technology is developed, deployed, and used. At the broad overview level, IT objective implies knowing the organization's goals and objectives, its core capabilities, and its critical success factors. Knowledge about the organization also includes knowledge about its environment and the constraints imposed on it by its suppliers, buyers, and competitors.

Hypothesis 4, Supported: There were significantly “strongly agree” and “agree” more than “not sure” as Likert response scale which business compensated concentration on the ability of their MIS department to understand and use VPN for security and protection. The result from these business respondents could provide evidence and sustain that VPN usage has a significantly effect on MIS protection.

Hypothesis 5, Supported: The result from these business respondents could provide evidence and sustain that VPN usage has a significantly effect on business competitive advantage. From an operational perspective, investments in information security by organizations willing to successfully embrace technology have resulted in increased efficiencies, cost reductions, global expansion, improved intra-company and customer communications, improved reporting and tracking methods, and increased competitive advantage in the marketplace.

Hypothesis 6, Supported: there were insignificantly “strongly agree” and “agree’ more than “not sure” in Likert response scale which business compensated concentration on their organizations ability to anticipate future changes and growth as perditions in VPN system capability, to chose information security technology that can accommodate this change and to efficiently mange the resulting technology change and growth. Business executive could distinguish the different after the implementation of VPN. The result from this question 15 could verify that the variation business objectives can significantly predict system capability such as implementation of VPN.

Hypothesis 7, Supported: there were significantly "strongly agree" and "agree" more than disagree which this question could sustain MIS security can significantly predict organization competitive advantage. This study has examined how innovation in information security such as VPN has sustained and facilitated enterprises to gain competitive advantage.

In this study, author used combinations mix approaches (quantitative and qualitative) within the research design. The use of a triangulated design is, however, far more complex than simply an aggregation of data collection strategies. The process of triangulation became characterised by the combination of sub-research questions in each phase including empirical , descriptive, and Interpretive (see figure 5.8). In this way, research sub-questions could contrast between phase one, phase two, and phase three. In tables 5.61 – 5.63 illustrate results in each pair of research sub-questions between phase one and phase two, phase two and phase three respectively including security perspective between bsuiness and IT.

Table 5.61 Empirical and Interpretive

Empirical Vs. Interpretive	Security Perspective
EQ.1 & IQ.1	VPN protocols can be used to secure and protect information systems. VPN users believed that they could configure connections to a VPN server, start connections, enrol for certificates to authenticate connections to VPN servers, and display events from the log.
EQ.2 & IQ.1	Business perceive operational costs reduction is important objective in their AHP ratio-scale as result because of VPN makes use of public network resources, business enterprise need not to buy its own networking equipment to cover remote user. A service costs less and delivers high-speed, secure connectivity to every branch location. MIS security can significantly predict organization competitive advantage.
EQ.3 &.IQ.1	IT professional perceive quality of service is important objective in their AHP ratio-scale as result because the ability for VPN protocol to obtain the network service it requires for successful operation. VPN offer classes of service and quality of service (QoS) guarantee as the traffic remains within the domain of one network operator and the security afforded by traffic separation is comparable with traditional unencrypted solutions such as frame relay. VPN users believed that they could configure connections to a VPN server, start connections, enrol for certificates to authenticate connections to VPN servers, and display events

	from the log.
EQ.1 & IQ.2	Business perceive tunnelling and authentication is important objective in their AHP ratio-scale as result because of establishment of data encrypted tunnel between their site and third parties (e.g. distributors, suppliers) and authenticates network user (identifying the user). VPN users believed that they could manage security keys for encryption and decryption for example, authenticating, encrypting, and decrypting data through the tunnel.
EQ.2 & IQ.2	IP security allows business people to access database server if they are as travelling or home remote user access can gain access to company intranet from a wide range of locations including home. VPN user believed that he or she could use safely removes the VPN Client software from his or her system and retains his or her connection and certificate configurations.
EQ.3 & IQ.2	IT perceive scalability is important objective in their AHP ratio-scale as result because A VPN platform should provide an upgrade path for supporting more users, as well as, for integrating new security services, such as virus protection and content filtering. Business distinguished different from IT because Scalability was more in technique skill which allows IT people to upgrade VPN systems easier. VPN users believed that they could transmit sensitive information over the Internet without needing to worry about who might see it.
EQ.1 & IQ.3	Business and IT perceive LAN access is important objective in their AHP ratio-scale as result because using a dial-up line to connect a branch office to a corporate LAN. The VPN software uses the connection to the local ISP (Internet Service Provide) to create a VPN between the branch office router and the corporate hub router across the Internet. VPN user could provide evidence and sustain that VPN usage has a significantly effect on MIS protection.
EQ.2 & IQ.3	Business and IT staff could make judgments about the importance of business objectives for optimal security assurance. VPN user believed that MIS security can significantly predict organization competitive advantage.
EQ.3 & IQ.3	The main objective was to provide decision makers (business and IT) with a set of validated and structured criteria for VPN protocols, considerable selecting the best information security technology features in decision-making. Both business and IT people had weighted VPN protocols in different perspective of information security features. VPN users believe VPN protocols provide user authentication and making sure users are who they say they are, by usernames, group names and passwords.

Table 5.62 Descriptive and Interpretive

Descriptive Vs. Interpretive	Security Perspective
DQ.1 & IQ.1	IT professional didn't think their organizations gain competitive advantage on information security technology when comparing with competitors because there was no information security technology existing in their organization in the past. VPN users believed that they could configure connections to a VPN server, start connections, enrol for certificates to authenticate connections to VPN servers, and display events from the log.
DQ.2 & IQ.1	Business compensated concentration on the improvement and gain competitive advantage after the implementation of VPN as their perdition of VPN implementation. Business executive could distinguish the different after the implementation of VPN. MIS security can significantly predict organization competitive advantage.
DQ.3 & IQ.1	Business respondent believed that their organization's ability to share information throughout the organization through effective VPN and communication platforms. VPN users believed that they could configure connections to a VPN server, start connections, enrol for certificates to authenticate connections to VPN servers, and display events from the log.
DQ.1 & IQ.2	Business respondent believed that the ability of their MIS department to understand and use VPN for security and protection. VPN users believed that they could manage security keys for encryption and decryption for example, authenticating, encrypting, and decrypting data through the tunnel.
DQ.2 & IQ.2	IT professional believed that their organization's ability to share information throughout the organization through effective VPN and communication platforms. VPN users believed that they could transmit sensitive information over the Internet without needing to worry about who might see it.
DQ.3 & IQ.2	IT respondent believed that their organizations ability to anticipate future changes and growth, to chose information security technology that can accommodate this change and to efficiently mange the resulting technology change and growth. VPN user believed that he or she could use safely removes the VPN Client software from his or her system and retains his or her connection and certificate configurations.
DQ.1 & IQ.3	Business believed that VPN is not only secure and their organization can gain competitive advantage. VPN user could provide evidence and sustain that VPN usage has a significantly effect on MIS protection.
DQ.2 &. IQ.3	Their organization ability to develop and experiment with

	VPN, which enable business processing and performance to take advantage of VPN and trends. The ability of their MIS department to understand and use VPN for security and protection. VPN user believed that MIS security can significantly predict organization competitive advantage.
DQ.3 &. IQ.3	Their organization's ability to share information throughout the organization through effective VPN Their organizations ability to anticipate future change and growth, to chose information security technology that can accommodate this change and to efficiently mange the resulting information security technology change and growth. VPN users believe VPN protocols provide user authentication and making sure users are who they say they are, by usernames, group names and passwords.

Table 5.63 Empirical and Descriptive

Empirical Vs. Descriptive	Evidence
EQ.1 & DQ.1	VPN protocols can be used to secure and protect information systems. IT respondent didn't think their organizations gain competitive advantage on information security technology when comparing with competitors because there was no information security technology existing in their organization in the past.
EQ.2 &. DQ.1	Business perceive operational costs reduction is important objective in their AHP ratio-scale as result because of VPN makes use of public network resources, business enterprise need not to buy its own networking equipment to cover remote user. Business compensated concentration on the improvement and gain competitive advantage after the implementation of VPN as their perdition of VPN implementation. Business executive could distinguish the different after the implementation of VPN.
EQ.3 & DQ.1	IT professional perceive quality of service is important objective in their AHP ratio-scale as result because the ability for VPN protocol to obtain the network service it requires for successful operation. VPN offer classes of service and quality of service (QoS) guarantee as the traffic remains within the domain of one network operator and the security afforded by traffic separation is comparable with traditional unencrypted solutions such as frame relay. Business respondent believed that their organization's ability to share information throughout the organization through effective VPN and communication platforms.
EQ.1 &. DQ.2	Business perceive tunnelling and authentication is important objective in their AHP ratio-scale as result because of establishment of data encrypted tunnel between their site and

	third parties (e.g. distributors, suppliers) and authenticates network user (identifying the user). Business respondent believed that the ability of their MIS department to understand and use VPN for security and protection.
EQ.2 &. DQ.2	IP security allows business people to access database server if they are as travelling or home remote user access can gain access to company intranet from a wide range of locations including home. IT professional believed that their organization's ability to share information throughout the organization through effective VPN and communication platforms.
EQ.3 & DQ.2	IT perceive scalability is important objective in their AHP ratio-scale as result because A VPN platform should provide an upgrade path for supporting more users, as well as, for integrating new security services, such as virus protection and content filtering. Business distinguished different from IT because Scalability was more in technique skill which allows IT people to upgrade VPN systems easier. IT respondent believed that their organizations ability to anticipate future changes and growth, to chose information security technology that can accommodate this change and to efficiently mange the resulting technology change and growth.
EQ.1 &. DQ.3	Business and IT perceive LAN access is important objective in their AHP ratio-scale as result because using a dial-up line to connect a branch office to a corporate LAN. The VPN software uses the connection to the local ISP (Internet Service Provide) to create a VPN between the branch office router and the corporate hub router across the Internet. Business believed that VPN is not only secure and their organization can gain competitive advantage.
EQ.2 & DQ.3	Business and IT staff could make judgments about the importance of business objectives for optimal security assurance. Their organization ability to develop and experiment with VPN, which enable business processing and performance to take advantage of VPN and trends. The ability of their MIS department to understand and use VPN for security and protection.
EQ.3 & DQ.3	Their organization's ability to share information throughout the organization through effective VPN Their organizations ability to anticipate future change and growth, to chose information security technology that can accommodate this change and to efficiently mange the resulting information security technology change and growth. Their organization's ability to share information throughout the organization through effective VPN Their organizations ability to anticipate future change and growth, to chose information security technology that can

	accommodate this change and to efficiently mange the resulting information security technology change and growth.

5.2.3 Summary

This study examined the factors that affect information security success by using triangulation research model that was developed from business and IT, an exploratory survey, VPN observation and interviews. Implementation success factors were used to help understand why the VPN implementation factors affected the system success and ultimate success from the use of the security system. As predictors are added to the model, each predictor can explain some of the variance in the dependent (VPN protocol) variable simply due to chance. One could continue to add predictors to the model which would continue to improve the ability of the predictors to explain the dependent variable, although some of this increase in R-square would be simply due to chance variation in that particular sample.

In these three phases, business and IT professional had significant relationships with perceived net benefits and explained a good portion of the construct's variance. These results illustrate that the effectiveness and efficiency information security that it provides are associated with the competitive advantage as perceived by the organization's data processing. In other words, effectiveness and efficiency information security can protect and secure data which allow organization to have secure environment and improve business processing. This study furthers the knowledge of business and IT success by supporting the use of multiple success dimensions and confirming other research findings that show the success dimensions (e.g., VPN implementation, data security, and perceived net benefits) to be interrelated. VPN implementation and business process do affect perceived net benefits in the context of business competitive advantage.

Business and IT professional are key ingredients to supporting the change business process and decision making in organizations. This finding is consistent with other IT implementation studies that substantiate the value of these organizational factors. VPN implementation is an expensive, enterprise-wide endeavour with significant organizational impacts. VPN as security technology creates changes that resonate throughout the entire organization, and it demands broad-based and lasting support. It requires the sponsorship and support of senior management; managers in the business units, and IT, there must be a substantial initial and ongoing commitment of financial and human resources. This commitment must be made while recognizing that the greatest benefits from VPN usually occur later rather than immediately. Together, all three phases' factors were found to be significant in the triangulation research model, and together they provide organizations with effective mechanisms for increasing widespread support for information security technology,

addressing politics, and ensuring that the necessary resources are provided. Interestingly, VPN implementation could influence business process and performance which allowed organization to gain competitive advantage and existing as champion for long time. Although studies have found that VPN user participation must follow organization security policy which can facilitate organization expectations and goal, this may be sufficient for the acceptance of VPN within the organization. All of these findings highlight some of the challenges that business and VPN user should expect when working with VPN as security technology.

According to the findings, having VPN, appropriate business and IT professional in the organization, and VPN user participation have positive effects on competitive advantage as outcome. Unfortunately, companies sometimes experience problems in these areas. The implementation of VPN demands a large financial investment that can be difficult management for approving without having guaranteed up-front tangible benefits. VPN user participation also can be challenging because the needs of many, diverse internal groups (e.g., marketing, production) must be understood and achieved the organization goal. Much information security literature advocates an incremental approach when implement VPN, which means implement VPN can take three- to six-month increments that each deliver substantial value to the business. In this way, business and IT can work toward goals that are more manageable in size, VPN users can participate in only relevant parts of the organization, and management can be satisfied that the information security technology is delivering high value and secure environment. If management requires post-implementation assessments of its investments, the value that is created during beginning increments can be used as a foundation for a rigorous future cost-benefit analysis. The findings suggest that most of the traditional factors from the implementation literature also affect the success of VPN, thus providing further evidence of the existence of a common set of IT implementation factors. Another contribution of this study is the way in which implementation success factors can be grouped together into organizational and technical success to more clearly communicate the kinds of effects implementation factors can have.

To the extent that the study could find any origins for IT visions, they seemed to be created as following: either through sustained communication between a group of IT and business executives or by fiat from a senior business person with IT credibility. A future study that looked only at the creation of IT vision could pay more attention to both processes and individuals. Different methodologies such participant observation or a large survey could be tried to see if the process of creating vision or the factors that accompany it can be

identified. In addition, it will be important to carefully identify the characteristics of an IT vision in order to interview or survey respondents.

The most important direct predictor of configuration in this study was a high level of communication between IT and business executives. However, one cannot mandate meaningful communication between individuals. IT people have to earn the right to play a meaningful role in management forums. Based on findings from this study, one important way for an IT professional to be heard is for him/her to devote the time necessary to develop business knowledge, the most influential construct in the research model. An IT professional needs to understand the leverage points of the industry, the history and current issues of the business units, and to learn to apply common sense in the application of technology to business problems. This change in view would help focus their attention on those information security technology and ideas that could produce the most benefit, rather than those that offer the most technical promise.

Line managers who have a deep knowledge both of the core business and applications of IT are the catalysts around which IT innovations seem to occur. In organizations where IT is critical to success, managers should be expected to exert the same influence over IT projects as they do over marketing and new product development. Organizations must recognize that IT knowledge is a core competence for managers; therefore, management training programs should include year's tour of duty working on a large information security project. The other aspect awareness of new information technology can be fostered by attendance at IT presentations. Over time, the level of IT competence within the organization will grow, enabling most managers to participate fully in IT decision making.

The importance of regular communication between IT and business executives cannot be overemphasized. Organizations must realize, however, that without some background of security technology perspective or shared beliefs, mechanisms such as IT steering committees may degrade into IT project review or budget approval committees. A strategic focus should be forged early in these committees, even though this process may reveal conflicting views about the role of IT within the company. Data from this study suggest a steering committee that isolates business and IT objective and discussion from other organizational issues may be counterproductive and could affect competitive advantage and organization goal.

5.3 CONCLUSION

This chapter had used triangulation research model as data collecting from three different sites and illustrated in three different phases by using business and IT professional as information security perception and competitive advantage. These phases corresponded to the different data type that were collected and the unique sub-questions that related to each data type. In this phase one, the used analytical hierarchy process (AHP) method, which would help business and IT staff of the organization structure their objectives in a hierarchic framework. AHP ratio-scale could illustrate business objective bias can significantly predict systems capability such as VPN security technology. The outcome of the analysis could advise IT objective can significantly improved business performance by using VPN system in their organizations.

Descriptive statistics were used to describe the basic features of the data in phase two. They provide simple summaries about the sample and the measures on competitive advantage as descriptive in triangulation method. With descriptive statistics author could simply describing what was or what the data shows. The interviews of VPN user and observation had used to support as additional in this study. The researcher asked VPN user at work place for some additional information concerning VPN security technology, especially with regard to the business and IT professional. Business and IT are two different sets of data which need to measurement scales. The measurement scales used should be at least interval scales, but other correlation coefficients are available to handle other types of data.

The rationale for the factors and the relationships among the factors can be described in the chapter 6. The relationship between business and IT professional, such as management support and user participation, are proposed to influence the success of the VPN implementation, which has been broken down into three unique facets as phases one through three. In next chapter will be described the factors that affect information security success by using triangulation research model that was developed from business and IT, an exploratory survey, VPN observation and interviews. Implementation success factors were used to help understand why the VPN implementation factors affected the system success and ultimate success from the use of the security system. This study furthers the knowledge of business and IT success by supporting the use of multiple success dimensions and confirming other research findings that show the success dimensions (e.g., VPN implementation, data security, and perceived net benefits) to be interrelated. VPN implementation and business process do affect perceived net benefits in the context of business competitive advantage.

CHAPTER 6
DISCUSSION OF FINDINGS

6.0 INTRODUCTION

This research has used nine research sub-questions that were grouped into three different phases. The findings of this study provide a detailed account of the role that business and IT professionals play in the creation and sharing of organizational knowledge within the context of information security technology. The inclusion of business competitive advantage as a factor influencing IT performance has positioned this work in a group of publications that argue for the beneficial relationship of business and IT. This knowledge enables business and IT professionals to see the big picture of information security in their current organization, to make linkages between different organizational units, and ensures focus on a larger perspective needed to extract benefits from the potential fit between the business and IT within the organizational context. It represents a holistic view of the organization and its current activities. This chapter presents revisits each phase, the research question and discusses the theoretical findings of the study. The hybrid research approach is also discussed and advocated to be a viable approach to complex problems in complex contexts. Finally, the results and the implications of the study are presented and some concluding comments offered.

An important contribution of this study makes is the identification of business and IT perspectives on information security technology. By establishing the link between business and IT, the study focuses and evaluates Virtual Private Networks (VPN) as an information security technology to find out if VPN can secure and gain competitive advantage by partisan business process and organization performance. This study articulates distinctive characteristics of Virtual Private Network and the management processes that extend the range of applicability across diverse business segments. It distinguishes between business and IT and explains why the exploitation of a complementary set of related information security artefacts (such as VPN) across multiple functions, create competitive advantage.

The most important direct predictor from this study was the high level of communication between business and IT. However, one cannot mandate meaningful communication between individuals. IT people have to earn the right to play a meaningful role in management forums. Based on findings from this study, one important way for an IT person to be heard is for him/her to devote the time necessary to create competitive advantage

and develop shared domain knowledge, the most influential construct in the research model. An IT person needs to understand the leverage points of the industry, the history and current issues of the business units, and to learn to apply business oriented constructs in the application of technology to business problems. This change in view would help focus their attention on security technology and ideas that could produce the most benefit and create competitive advantage, rather than those that offer the most technical promise.

6.1 PHASE ONE: EMPIRICAL

In phase one the analytical hierarchy process (AHP) method was used to help business and IT staff of the organization structure their objectives in a hierarchic framework. Answers to the research sub-questions as following: What measures are critical for MIS security? , and What is the relationship between IT and Business objectives for optimal security assurance?, and In what ways can the VPN improve the performance of the employees and managers in an organisation? The study provided evidence in support of the existence and performance effects of using VPN as information security technology. While it may be appropriate to impose consistent IT strategies and consistent information security technology solutions onto business units operating in different industries, it is better to use common information security technology and to coordinate the strategic IT decisions of the business units by using common IT strategy making, IT human resource management, and IT vendor management processes. It is up to the executive management to coordinate IT vendor relationships. Pooling of the negotiations and implementing information all security technology, will increase the quality of information security, and make IT audit a priority. Likewise, it may not be surprising that the use of a common IT-HR management process reduces recruitment and training costs, or that the use of a common IT strategy-making process reduces the administrative costs of IT strategy making and enhances coordination of IT strategies.

In phase one, the VPN system research explored the implementation feasibility of the network traffic scheme, and identified potential demands from business and IT professionals. The goal of the VPN implementation is to provide a remote employee with the resources and security of the corporate LAN from their remote site through the Internet. This study found that the VPN's performance has become a significant issue in its business applications because the encrypted packets impose more traffic loads into the Internet and costs in the organisation gaining the benefits from the VPN. According to VPN user observation, they have VPN solutions that enables strong authentication of users and devices via digital

certificates to help provide protection from hackers or attempts to impersonate legitimate users. This solution offers flexibility in how digital certificates are stored and used. Digital certificates can be stored encrypted on the user's computer, smart card, USB token or made available through a secure credential server. In phase one, business and VPN users showed that the VPN possesses some useful business features such as user authentication and user account management that make the implementation of traffic feasible and secure the environment. Business and IT professionals found and weighted IPSec more important for connecting geographically distributed LANs into a virtual intranet/extranet over the Internet.

According to business, VPN enables enterprises to contain costs, enhance security, and expand access and availability, while enhancing their business processes and improving customer service and best practices. VPN delivered secure, reliable, ubiquitous, business wide connectivity over a shared network infrastructure, using the same access policies as private networks. Many small and medium-sized businesses turn to VPN to cut costs and become nimble in the competitive marketplace. At the same time, they benefit from improved network performance and VPN-enabled applications such as IP communications. VPNs also enable cost-effective, secure remote access to networked resources. It is optimal for businesses with mobile workforces and telecommuting employees, and also a necessity to provide business partners and customers, too, with instant access to relevant business-critical data and applications while ensuring privacy and security. Remote-access VPNs securely connect users to businesses over dialup, ISDN, DSL, cable, and wireless technologies. According to market research enterprise The Yankee Group, business applications that support processes such as finance, human resources, collaboration, and communication are central to the strategies of small and medium-sized businesses. For this reason, many businesses turn to service providers that can supply not only the VPN network infrastructure and ongoing management, but also a full range of value-added services that operate transparently over VPN.

Without the VPN, the employee would have to be physically present at headquarters in order to access the corporate LAN. Thus, a VPN gives employees considerable flexibility while away from corporate headquarters and provides them with access to critical corporate resources at remote locations, which previously were not available. In setting up a secure VPN, a company usually has established a VPN server at company headquarters that can be the base point for remote employees' connections. The VPN server can be installed with different types of VPN software. Employees can also be given VPN client software for their

computers out in the field. A common VPN implementation is to give the employee a company laptop with client VPN software installed and to outsource the hosting to an ISP.

In the research findings, companies used VPN as the logical solution for establishing secure, end-to-end private network connections over a public networking infrastructure. Remote-access VPN enabled business to reduce communications expenses by using the local dialup infrastructures of Internet Service Providers. At the same time, VPN allowed the business, telecommuters, partners, and day extenders to take advantage of broadband connectivity. Realizing their full benefit required a robust, highly available VPN solution. Both business and IT professionals weighted and found IPSec is more important than the other two protocols. IP Security (IPSec) VPN provides the most robust remote-access environment to remote users by securely extending almost any data, voice, or video application to remote working locations. IPSec VPN client software on the remote system enables a user experience and workflow consistent with the office environment by providing easy application access and system integrity enforcement. IPSec VPN thus extends the productivity of the office to virtually any location. Its "any application access" has made IPSec VPN the de facto standard for extending connectivity to home offices, travelling employees, remote workers, and day extenders.

The optimal performance of information security technology may entail actions such as physically moving IT people into an MIS department and business units, and allowing business and IT people working together to improve business process and organization. These strategies can help gain better tactical positioning and strategic competitive advantages. Systems analysts can be encouraged to follow their applications into line areas, either temporarily or permanently. Other approaches would include bringing business executives into senior IT roles. All of these activities would be designed to change first the behaviours and second the attitudes of IT professionals toward the needs and the priorities of the business. Changes in hiring practices, assignments, and rewards must be put in place to reinforce the message that IT is an integral part of the business.

Executive management who have a deep knowledge both of the core business and applications of IT are the catalysts around which IT innovations can to occur. In organizations where IT is critical to success, managers should be expected to exert the same influence over IT projects as they do over marketing and new product development. Organizations must recognize that IT knowledge can be core capability for managers. The perspective of business and IT professionals can be shared and developed through organization functions. IT knowledge identified in this study was the ability to implement an

important information security technology. The other aspect was awareness of information security technology can be fostered by perspective negotiation between business and IT professionals. Over time, the level of IT competence within the organization will grow, enabling most managers to participate fully in both business and IT decision making.

An important implication of this study is for the information security technology evaluation and analysis of strategic importance of business process and information security. The information security technology evaluation and analysis assesses the strategic importance of a given security perception by examining business and IT perspectives. This study uncovers and conenterprises business and IT perspectives on VPN. The analyses show how misleading results in the context of interconnected, complementary niches can occur (eg. Overstated performances relative to the enterprise measures). For example, evaluation of VPN technology may suggest that an organization can obtain competitive advantage with its use but the question of how it is used and how it is implemented has not been answered if the organisation is looking for maximum benefits. In this study it was found that VPN technology complements business requirements such as IT strategy-making processes, IT-HR management processes, and IT vendor management processes. The evaluation of information security technology in all respects is critical for maximising the business process and organization performance. Thus, this study generates an important new insight for information security of the strategic importance of possessions. Information security technology is not strategic on its own and gains strategic significance as part of a complementary system of possessions. In assessing the strategic importance of information security technology, evaluation of information security should consider complementarities of the resource with other resources, and if complementarities exist, the analysis should focus on the business process, organization performance, competitive advantage, and non-substitutability attributes of the whole system of complementary possessions rather than on the attributes of each resource in isolation.

6.2 PHASE TWO: DESCRIPTIVE

Phase two investigated and answered sub questions as following: (i) in what ways can a more efficient computer security system benefit the overall organisation competitive advantage? (ii) What is the relationship between MIS security and competitive advantage? (iii) In what ways can VPN provide cost advantage? This study has examined how innovation in information security such as VPN has sustained and facilitated enterprises to gain competitive advantage. From an operational perspective, investments in information security

by organizations willing to successfully embrace technology have resulted in increased efficiencies, cost reductions, global expansion, improved intra-company and customer communications, improved reporting and tracking methods, and increased competitive advantage in the marketplace. Security is the main issue facing companies with remote access. Employees in the field, such as salespeople or telecommuters, have access to mission critical data and pose a significant threat to organizational systems security. There are numerous potential breaches of security related to remote access devices such as VPN and laptop computers that can be misplaced, stolen or damaged. The challenge facing information security is to protect sensitive company data, enable secure remote access, and provide user-friendly and productive electronic tools for its mobile workforce. IT must also implement an education process for training employees not to use unauthorized devices or install any unauthorized programs that might threaten the integrity of company data.

While this approach to studying the competitive advantage of information security has much to recommend it, it has at least one important limitation. With few exceptions, this approach has focused on what is, in fact, a highly aggregated dependent variable, namely, enterprise performance. For example, because enterprises can have competitive advantages in some business activities and competitive disadvantages in others, examining the relationship between information securities associated with different processes within an enterprise and an enterprise's overall performance can lead to misleading conclusions. Also, an enterprise may have competitive advantages in some business activities, but various stakeholders may have appropriated the profits these competitive advantages might have generated before they can affect a enterprise's overall performance. Also an enterprise may have resources that have the potential for generating competitive advantages but has not fully realized this potential through its businesses activities.

The descriptive findings presented in this section suggest that, in fact, enterprises may protect information assets and possess competitive advantages at the level of business processes that are not reflected in an enterprise's overall performance. If competitive advantages in one business process are offset by competitive disadvantages in other business processes, or if any profits generated by a enterprise's business process are appropriated by a enterprise's boards and not reflected in a enterprise's overall performance, there may be no relationship between the valuable, and capabilities that enable a enterprise to gain competitive advantages from a particular business process and a enterprise's overall performance. As important, the results presented also constitute a test of information security logic at the protection of information system and business process unit of analysis. Results

reported here are consistent with VPN as information technology expectations. Intangible and socially complex capabilities-service climate and managerial IT knowledge-are positively related to customer service performance. Tangible and non-socially complex information security technology and investment in customer service do not seem to explain variation in customer service performance.

Evidently, these results do not mean that enterprises should not invest in information security technology and other tangible aspect of business and IT professional. Clearly, these kinds of resources are required if an enterprise is to have secure and effective operation. However, because these resources are not costly to replicate, most enterprises in a mature industry like the telecommunication industry will already have them in place, and thus they will not be a source of competitive advantage. Only those resources that are costly to imitate-operation climate and managerial business and IT perspective on information technology are likely to continue to provide competitive advantages for enterprises, and thus only these resources are related to information security and business process. Thus, this study also extends the growing number of empirical tests of information security logic.

This study recognizes important common ground between these business and IT perspectives on information security such as VPN. On the one hand, this phase acknowledges that resources and capabilities that are not translated into information security, activities, routines, or business processes cannot have a positive impact on an enterprise's performance. Information security, activities, routines, and business processes are the mechanisms through which resources and capabilities get exposed to market processes where their ultimate value and ability to generate competitive advantages are realized. Alternatively, this study also recognizes that the ability of enterprises to pursue certain effective security, activities, routines, or business processes may be limited by the resources and capabilities they control. That is, enterprises are not 'empty canvasses' upon which any information security, activity, routine, or business process can be drawn, and the differential effectiveness of these enterprise processes depends critically on the resources and capabilities a enterprise possesses.

Certainly, the research reported here not only recognizes this common ground, but suggests that understanding the relationship between a enterprise's resources and the effectiveness of information security, activities, routines, or business processes is particularly fruitful ground for analysing the empirical implications of information system theory. Thus, adopting a disaggregated dependent variable not only facilitates the theoretical and empirical

integration of two previously competing perspectives in the strategic management literature, but it also facilitates the testing of information security logic.

This theoretical integration has implications that move well beyond the reported research. For example, the argument has examined how an enterprise's resources and capabilities can condition its ability to implement specific information security, activities, routines, or business processes. However, an enterprise's information security, activities, routines, or business processes could also be an important determinant of an enterprise's resources and capabilities. In this sense, prior information security, activities, routines, and business practices can become part of the path-dependent process through which an enterprise develops its resources and capabilities, which in turn condition its ability to implement future activities, routines, and business practices. From the perspective of business and IT professional, research on understanding why information security, activities, routines, or business practices are able to generate competitive advantages while others cannot is likely to be more helpful than research that examines just the relationship between resources and enterprise performance at a more aggregate level. By focusing on information security, activities, routines, and business processes where resources are deployed and where their first-order effects are expected to be realized, business and IT professional might be in a better position to benchmark the resource endowment of their enterprises and identify critical resources that should be exploited, developed, and protected. And while a enterprise may have limited ability to change its endowment of resources in the short to medium term, management may have the ability to redesign some of a enterprise's information security and business processes to more efficiently and effectively exploit resources and capabilities it already possesses. In this sense, integrating these previously competing explanations of enterprise performance may ultimately enhance the applicability of the field of strategic management.

This study provides evidence in support of the existence and performance effects of using VPN as information security technology. While it may be appropriate to impose consistent IT strategies and consistent information security technology solutions onto business units operating in different industries, it is also appropriate to use common information security technology and to coordinate the strategic IT decisions of the business units by using common IT strategy making, IT human resource management, and IT vendor management processes. It may accommodating to executive managements who are the coordination of IT vendor relationships pools the negotiation and implementing information security technology, and increases the quality of information security, and IT audit. Likewise,

it may not be surprising that the use of a common IT-HR management process reduces recruitment and training costs, or that the use of a common IT strategy-making process reduces the administrative costs of IT strategy making and enhances coordination of IT strategies. What is likely to be unexpected to executive management is that, when taken in isolation, these activities do not have any noticeable impact on the corporate performance of the enterprise. These activities complement and reinforce each other. The absence or weakness of one of them weakens the benefits obtained from the others. It is critical for executive management to attain the competitive advantage and become in superior position and better than competitors.

However, executive management should be cautious in pursuing competitive advantage as the diversification levels of their enterprises increase. Although the association between information security technology and enterprise performance remains positive at increasing levels of diversification, the strength of the association weakens. The increasing level of diversification may raise implementation barriers to the creation and exploitation of information security competitive advantage. IT professional may face technical, political, and financial barriers, especially when the enterprise diversifies through mergers and acquisitions. It may be risky to try to implant a system of mutually reinforcing IT management activities into the new businesses. Complementarities among the activities may increase the risk of implementation failures. Failure in one activity may lead to failures in others as well. Before pursuing effective and efficiency of information security technology, executive management should carefully assess the potential risks and costs, especially at higher levels of implementation.

This study also finds that the use of a centralized, decentralized, or hybrid mode of IT governance make a significant difference in the relationship between information security technology and enterprise performance. Contrary to conventional wisdom, the formal locus of business and IT perspectives and decision making may be the dominant contingency in exploiting the performance effects of information security technology such as VPN.

6.3 PHASE THREE: INTERPRETIVE

In phase three, there are three research sub-questions which used for VPN user observation. There are (i) What intangible MIS elements contribute to business value delivery? (ii) What organisational capabilities are enhanced by effective MIS security? (iii) What organisational capabilities are enhanced by effective MIS security? Observation of the effectiveness of information security needs an additional issue to sustain in this study. The purpose of

conducting such tests is to evaluate the VPN and observe VPN user how the different functionality factors play a role in its performance. The ability for VPN users to outsource their networks to a service provider is a key benefit and attraction for user to adopt VPN services. The service provider would be responsible for the management and operation of the business process. The attraction for a VPN user would be that it allows them to concentrate and focus on their core business such as finance or marketing and leave the operator responsible for their telecommunication infrastructure. In fact that VPN networks would allow remote, location independent access and connectivity to the network makes VPN service attractive for customers who have remote access within their organization.

During the VPN observations, the researcher noticed that potential VPN users have to make a request why they need VPN access and they need to get proper approval for this usage from senior management. Just because a company supports VPN usage does not mean usage should be given out to any employee who desires it. The Researcher found out that VPN users should also be given the minimal amount of VPN lifetime that they would require for their job duties. Once an employee has been approved by management for access to VPN capabilities, the VPN administrator should decide what protocols and software the user can utilize over the VPN. The user can allow protocols that pertain to his or her job function and nothing more.

In this study, it was found that companies have not allowed users to access VPN from their own personal computers. As discussed in the section on coping theory, the assessment of an information security technology event starts with primary appraisal. At this stage, the user determines the expected consequences of the information security technology, such as VPN, event and how they are likely to affect him/her both personally and professionally. For example, a user might think that a new system will make her job less tedious and more interesting and that she will need to learn new skills and to adapt her working procedures. Another user might be afraid of losing his job and think that he does not have the necessary skills to obtain a new and interesting job. There are several benefits to restricting access to company-owned computers as following. First, the user will not be able to mix confidential company data with personal data on a home computer. If a company allows VPN users to install VPN client software on their home personal computers, the company is at risk for receiving viruses and worms that may exist on the employees' home personal computers. Infected home computers are a serious vulnerability to a secure VPN. Second, when the user is terminated from VPN usage, the company simply needs to gather the laptop from the user rather than trust the user to erase VPN client software from a

personal computer. Third, it is easier for a VPN administrator to configure the same laptop type for all VPN users rather than attempt to configure all the varying types of personal computers users would have at home. Additionally, the laptops must have capabilities for remote software updating. This means that the VPN users should be able to implement security patches, O/S updates, and updated virus software from their remote sites.

Consider the case where a VPN user does not properly close a VPN session and begins browsing the Internet. The user downloads software that is infected with a virus. The virus then utilizes the established VPN session to send a copy to the corporate LAN. Scenarios like this are possible without updated protection software on the laptop. A VPN provides a secure connection from the VPN user to the server, but it does not analyse the content of the data inside packets. Insist on laptop security training for VPN users. If a hacker can steal a VPN user's personal laptop, he or she is very close to compromising the VPN network. VPN users should be made aware of proper laptop security. Laptop security should include proper laptop identification tags, preferably engraved in the laptop. Physical controls, such as cables and locks, should also be implemented. VPN users who receive company-owned laptops should be provided with nondescript carrying cases instead of laptop carrying cases with a company's or computer manufacturer's logo on them.

Enforce strict disconnection rules within the VPN. It is important to minimize VPN usage if at all possible. The more time a VPN user is connected to a VPN, the more the VPN is vulnerable to attack. Thus, strict disconnection rules should be enforced at all times. For example, a security policy might state that all VPN users will be disconnected after 15 minutes of inactivity and must authenticate again. Another issue to be aware of is what hardware VPN users will utilize for their connections from their remote sites. A user can connect to a VPN via a cable or dial-up modem, but now it is common to connect via a wireless network. It is extremely easy for a hacker to sniff wireless traffic. It is true that the packets are encrypted in a VPN, but the more packets a hacker can sniff; the more likely it is that the hacker can break the encryption in the VPN packets. By avoiding wireless VPN, a company takes great steps toward concealing its VPN packets from hackers.

All VPN usage should be well documented, including each user's name, time of VPN access, duration of VPN access, and resources used. The company should also monitor connection attempts, both successful and unsuccessful. By closely monitoring audit logs, the internal auditor can watch for suspicious VPN activity and VPN abuse. Third-party VPN auditing software is available, and many VPN software packages come with auditing software.

Moreover, this study predicts that VPN is capable when the conditions of full business implementation are met. Consistent with these predictions, the individual dimensions of information security technology are able to assemble organization security requirement and business and IT perspective. Organization security policy and management strategy depend on information technology security and realize VPN as a business instrument to gain competitive advantage and keep it in high position and value as an organization goal and achievement. However, the complementarities among the dimensions make information security technology relatedness a strategic resource that creates strategic advantages across business units and function, and improves corporate performance. Thus, this study extends perspective knowledge of business and IT professionals of diversification by uncovering that a complementary set of VPN could create competitive advantage over the competitor, assemble all business requirements and improve corporate performance.

6.4 IT PROFESSIONAL AND BUSINESS VALUE

The business environment where IT is used to gain business value, IT professionals must have an understanding of what their organization is about, that is, the business context in which technologies are developed, deployed, and used. At the broad overview level, knowledge of the organization implies knowing the organization's goals and objectives, its core capabilities, and its critical success factors. Knowledge about the organization also includes knowledge about its environment and the constraints imposed on it by its suppliers, buyers, the government, and competitors.

In this research, the researcher found that this area of knowledge addresses the need for IT professionals to proceed as business problem solvers and to integrate business development with IT capability. It refers to their ability to visualize the ways in which IT can contribute to organizational performance and to look for synergies between business and IT activities. It is the analytical thinking skills that enable an IT professional to understand clients' issues and needs, to see problems within a big-picture framework, and to conceptualize how parts and functions fit together. This understanding of the tight coupling between business and IT is implemented in the different phases of projects, from the initial analysis to the assessment of success.

IT professionals need to understand what the functional areas of their organization are, including their objectives and problems and business process. This internal view of the organization is concerned with an understanding of the business processes supported by IT, as well as an understanding of the connections and interdependencies among different

organizational units. IT professionals can develop a stronger understanding of the organization by feeling responsible for organizational performance that is beyond the direct impact of their specific area of work. This means that they need to think about and understand the development of the business as a functional area member would, and participate in making functional areas successful in the same way. There is an active component associated with this responsibility that refers the ability of IT professionals to learn about their business. This active role is taken by IT professionals in learning about their organization adds to the more static knowledge of the organization identified in other studies, and increases their general business knowledge specific to their organization.

The most important direct predictor of this study was a high level of communication between business and IT professionals. However, one cannot mandate meaningful communication between individuals. IT people have to be involved in business process and functions for support and better understanding in business roles. Information security analysts can be encouraged to follow their applications into line areas, either temporarily or permanently. Other approaches would include bringing non-IT people into senior IT roles or hiring junior analysts with a broad education. All of these activities would be designed to change first the behaviours and second the attitudes of IT professionals toward the needs and the priorities of the business. Changes in hiring practices, assignments, and rewards must be put in place to reinforce the message that IT is an integral part of the business.

At the conceptual level, this study focused on the contribution by IT professionals to their organizations with their business process. By enhancing their respective understanding of each other's domain, the development and effectiveness of their enterprises can be improved. The instrument developed and validated with this study, and the one in earlier work on IT knowledge for business people, should facilitate the investigation of a broader model. The expertise of IT professionals in their own domain can also be included to compare the relative contribution of their functional and cross-functional expertise to the development of enterprises.

6.5 SUMMARY

The purpose of this study was to draw on information security and competitive advantage of the enterprise to explicate the nature of an enterprise's information security technology capability and its relationship to business process. This study contributes to the growing body of literature linking business and IT which provides a framework for understanding how information security technology may be appropriately viewed as an organizational capability.

More importantly, it is one of the first studies to provide empirical, descriptive, and interpretive tests of business and IT professional perspective on VPN as information security technology. Viewed from business and IT perspective, the research findings indicate that information security technology capability is a rent generating resource that is not easily imitated or substituted. Isolating mechanisms such as time compression diseconomies, connectedness of resources, and social complexity allow enterprises with high information security capability to achieve and sustain superior performance.

It suggests that the inconsistent statistical findings about the relationship between business and IT which enterprise information security may be attributed to management incomplete understanding of the nature of a enterprise's security resources and skills and to the fact that IT investment dollars serves as a poor surrogate for assessing a enterprise's IT intensiveness. It is rare for businesses to develop security technologies in-house. Instead, they rely on a suite of products (technologies) bought from security vendors. The result is that the vast majority of technological innovation and new product development in the security field is being driven by vendors. Given the complexity associated with creating an enterprise wide IT capability, in any sample of IT spenders, only a small subset of the sample is likely to have the right IT resources in place for achieving competitive advantage. Other enterprises are more likely to have incurred the expenses of IT without comparative parity in IT capability.

By establishing the link between information security technology, such as VPN, capability and superior enterprise performance, the study serves to inform business managers that enterprises should do much more than merely invest in IT. They should identify ways to create an enterprise-wide information security technology capability. Through theoretical arguments and practical examples, this study shows why building such a capability is complex and requires time and effort. For business managers, however, there is little by way of guidance for developing information security technology capability, although more recently, an increasing number of studies have begun to address this issue.

The first step toward building any strong organizational capability is self-assessment, which requires enterprises to assess their own strengths and weaknesses. To identify and appraise an enterprise's information security technology capability, managers must look broadly and deeply. This study has relied on external peer evaluations of information security technology, such as VPN, capability and used the three phases ranking as a measure of an organization's information security technology capability. Perhaps managers would do well to compare themselves to other enterprises in their industry that get ranked as IT leaders and

understand the nature and scope of their IT resources. It is also critical to develop quantifiable measures of performance that permit inter-enterprise comparisons.

Benchmarking can also play an important role in upgrading organizational capabilities. Enterprises should identify activities or functions that need improving and then identify companies that are world leaders in those activities. Finally, the leverage of IT capability for competitive advantage is contingent on the sustenance and enhancement investments that enterprises have to make. Realistically, competing enterprises are likely to strive to bridge the resource and skill gaps that place them at a disadvantage relative to competition. In practice, however, enterprises fall into rigidity traps and face enormous organizational barriers in their efforts to change. Additionally, the IT staff in organizations had a vested interest in preserving the legacy systems and resisted organizational change. IT resources that were once valuable to these enterprises had been rendered obsolete and created a competitive disadvantage.

This study shows that the three phases are different patterns in streams of actions that are initiated by different appraisals and lead to different outcomes. From an individual point of view, all of the strategies can be effective in helping to address personally relevant issues raised by an IT event. For some, restoring emotional stability and reducing the stress associated with the IT event is a significant outcome that allows them to continue to work and function properly in an environment they had initially perceived as threatening. For others, pushing their limits further by learning to use information security technology will constitute a major achievement. Still others will grasp an opportunity to increase their productivity and overall performance. From an organizational point of view, the benefits satisficing and self-preservation strategies might at first appear suboptimal because individuals are not trying to maximize the potential benefits of an IT event. In some situations, however, inducing individuals to try to maximize IT benefits might require substantial organizational changes and investments (e.g., increasing job autonomy, decentralizing decision-making authority, extensive user training, or empowering users) that might outweigh the benefits an organization can achieve in doing so. On the other hand, although employees' ability to restore emotional stability is not an end in itself, it should not be overlooked. This might be a required step before they can perform problem-focused adaptation efforts which will eventually increase operational efficiency and effectiveness.

7.0 CONCLUSION

Results from this study also serve to inform the debate about the effectiveness and efficiency of information security. The advancement in research of triangulation is urged by the

increasing importance of business and IT perspective of information security technology knowledge in the organization. The research succeeded to identify the difference in perceptions between business and IT staff in evaluation of VPN protocol effectiveness. This study holds importance for professionals tasked with evaluating for company wide security deployment. As the area of information security gains increased importance due to the strategic role of technology in organizations, and current events impact areas such as disaster recovery and enterprise continuity planning, a study of end-users to determine their perceptions about information security controls in organizations is critical for protecting organizational assets. Evaluating information security is complex and a dynamic process; therefore bringing together the business and IT perspectives of information security evaluation may facilitate the process of knowledge sharing in the organization.

The nature of work for IT professionals is changing; interaction with people from other functional areas is now part of their work. IT professionals need to apply their technical knowledge in a way that is beneficial to the organization, and act cooperatively with their business partners. To succeed in this endeavour, IT professionals need a growing range of non-IT skills. The conclusion of this study stands out clearly: the knowledge that IT professionals have in the general business domain, and in the interpersonal and management domain, does matter in the protecting and secure the enterprises information assets including gain competitive advantage.

Another implication of this study is for the complementarity theoretic perspective on the business value of IT. Studies using this perspective focus mainly on complementarities between business and IT professionals. This study uncovers that complementarities among information security technology can create significant synergies and serve as a significant secure and source of business value and competitive advantage on their own. This study empirically demonstrates that super-additive business and IT value arising from the complementarity of information security technology and IT management processes have significant positive effects on corporate performance. Finally, this study makes an important methodological contribution to IS research. This study developed a hybrid approach for capturing information security technology such as Virtual Private Network (VPN) arising from business and IT perspective. This study also adds to the literature on partnerships between IT and business people. With higher levels of business knowledge, IT professionals also have higher intentions of developing further or strengthening their partnerships with their clients.

CHAPTER 7
RECOMMENDATIONS

7.0 THE CASE

The research reported in this study employs both quantitative and qualitative research methodologies within the quantitative paradigm to investigate the competitive advantage and information security technology user's perception of Virtual Private Network (VPN) functionality. Information security technologists and business scholars are motivated by a desire to understand how and to what extent the application of IT within enterprise systems leads to improved and secured organizational performance. The most important direct predictor of this study was a high level of communication and objective between business and IT professionals. In Chapter 5, business and IT staff had made judgments about the importance of VPN protocols which they used and the knowledge of the security subject matter. According to the results, business and IT had different perspectives with respect to operational costs reduction. Business respondents showed operational costs reduction was an important objective in their AHP ratio-scale. As a result they made use of public network resources, and the business enterprise did not buy its own networking equipment to cover a remote user. This service it was argued costs less and delivers high-speed, secure connectivity to every branch location. IT believed quality of service was an important objective in their AHP ratio-scale because the ability for VPN protocol to obtain the network service it required gave successful operations.

In phase two, the results for competitive advantage questions were discussed in chapter 5 for both business and IT. Business and IT professionals responded and clarified understandings of information security and competitive advantage. Implementation success factors were used to help understand why the VPN implementation factors affected the system success and ultimate success from the use of the security system. As predictors were added to the model, each predictor can explained some of the variance in the dependent (VPN protocol) variable simply due to chance. In this study, business and IT professionals had significant relationships with perceived net benefits and explained a good portion of the construct's variance. These results illustrate that the effectiveness and efficiency of information security are associated with the competitive advantage as perceived by the organization's data processing. In other words, effectiveness and efficiency information security can protect and secure data which allow organization to have a secure environment

and improve business processing. This study furthers the knowledge of business and IT success by supporting the use of multiple success dimensions and confirming other research findings that show the success dimensions to be interrelated. VPN implementation and business process do affect perceived net benefits in the context of business competitive advantage.

In phase three, the researcher had used observation and interview for additional information concerning VPN security technologies. When organizations exchange information to help facilitate business processes, the importance of privacy is well established and has become customary. An organization wants its information kept confidential to prevent damage that may occur if the information is obtained by competitors or other parties that could use the information to negatively impact the competitive position or the well-being of the information-providing company. The provider of the information has a public image to protect and the misuse of confidential information could result in bad publicity. In the case of publicly held companies, improper dissemination of proprietary information could negatively impact stock value. VPN users believed VPN enable their organizations to leverage the internet's cost-saving and flexibility, while protecting sensitive information. VPN provides the infrastructure to support the secure transmission of data across an organization's network. VPN users believed with the advent of affordable VPN implementation and deployment, their organization can by pass this expensive and complex remote access solution. They believed VPN delivers remote access via ubiquitous Internet connections. VPN remote access presents challenges in protection of the confidentiality and integrity of essential business information as it travels over the public Internet.

From the VPN user's perspective, VPN operates transparently, melding their computer desktop at home with the resources of the office network. VPN users used their network application and data as if they are sitting from of their computer in the office. Organizations have traditionally been able to justify the high-cost of security professional to implement and maintain their complex security and VPN requirements. They need security and VPN solutions which are strong enough to protect the network and provide secure remote access, but easy enough to set up and run for organizations with security environment. Centralized configuration, monitoring and distribution of security and VPN policies ensure a uniform security environment throughout the organization. Centralized security management also dramatically reduces security and VPN deployment and management costs. Business people believed VPN saves money because they use the Internet - not costly leased lines which can be transmitted information to and from authorized users.

7.1 THE ALIGNMENT ISSUE

Information security knowledge is defined here as the ability of business and IT professional, at a deep level, to understand and be able to participate in the others' key processes and to respect each other's unique contribution and challenges. This is the knowledge between business and IT perspectives on information security which enables organization to see the big picture of information security in their current organization, to make linkages between different organizational units, and ensure focus on a larger perspective needed to benefit from the potential fit between information security technology and the organizational context. It represents a holistic view of the organization and its current activities.

In a business environment where information security technology is used to protecting information and gain business value, business and IT professional must have an understanding of what their organization is about, that is, the business context in which technologies are developed, deployed, and used. At the broad overview level, knowledge of the organization implies knowing the organization's goals and objectives, its core capabilities, and its critical success factors. Knowledge about the organization also includes knowledge about its environment and the constraints imposed on it by its suppliers, buyers, the government, and competitors.

Therefore research model suggests that the organization capability of business and IT professional comprises knowledge of and skill in broad categories of organization-specific and interpersonal and management. In turn, each of these categories is formed by more specific areas of knowledge by evaluated information security technology. Organizational overview, organizational unit, organizational responsibility, and business-IT integration are said to form the organization-specific knowledge, while interpersonal communication skills, leadership skills, and knowledge networking form the interpersonal and management knowledge, suggesting a third-order model for organization capability.

In this study, the contribution of business and IT professionals to their organization with their perspective of information security technology such as VPN was examined through their intentions to engage and maintain gain competitive advantage. The organization capability of business and IT professional will influence such beliefs, and increase their awareness of the potential contributions of information security technology to business objectives hence providing the reason for partnering with business partners to put information security technology into effective and efficiency use.

7.2 PROTECTING INFORMATION

In this research, IT managers believed VPN maintains privacy through the use of tunneling protocols and standard security procedures. A secure VPN encrypts data before it travels through the public network and decrypts it at the receiving end. The encrypted information travels through a secure tunnel that connects to a company's gateway. The gateway then identifies the remote user and lets the user access only the information he or she is authorized to receive. A secure VPN can be used for the authorization of orders from suppliers, the forwarding of revised legal documents and many other confidential business processes. Recent improvements in VPN technology have also increased the system's reliability.

VPN users believed VPN enabled their organizations to utilize cost-effective Internet transport to connect remote offices and remote users to the main corporate site, thus eliminating expensive dedicated WAN links. For example, in this study, an insurance company provided underwriting and reinsurance services to clients nation wide from its base in Bangkok, Thailand. The 250 staff members at headquarters need to communicate with company subsidiaries. IT manager said that managing these communications was complex and expensive for company, until the company installed a Virtual Private Network (VPN). VPN has enabled company to reduce communication costs, streamline back office operations, and improve service to partners and clients.

Before the insurance company implemented a VPN, phone costs for staff dialing into the company network were high. In addition to domestic long distance phone calls, company was paying for long distance network access from staff located overseas. In addition, company spent large amounts of money on international faxes and shipping services. Since it began sharing information over its VPN, costs have dropped dramatically. For example, company used to spend more than $50,000 annually sending faxes to Asia. Since adding the VPN this expense has been virtually eliminated.

The insurance company has also benefited from the VPN assistance with technology support. Using the VPN, the company's Bangkok-based support staff is able to monitor remote servers, e-mail systems, Internet connections and software applications network-wide. When the e-mail server goes down in a headquarters, for example, the staff can analyze the problem using a home computer and can often correct it through the VPN. In addition, the company manages many of its back-office operations over the network, including billing, statement processing, claims, and general accounting.

Security is an issue for company on the Internet, but particularly because of the insurance data it handles. In the past, employees had to encrypt all information including e-mails that were sent over the public infrastructure. Using the VPN, company authorized users can send e-mail through its intranet, which is protected using IP Security protocol. The company also is now able to securely share information with clients over its private network.

The requirement that is common to secure VPN, trusted VPN, and business and IT is that the professional must know the limitations of the VPN. Regardless of the type of VPN in use, a VPN is meant to have capabilities that the regular network does not. Thus, IT professional must be able to know at all times what data will and will not be in the VPN. All traffic on the secure VPN must be encrypted and authenticated. Many of the protocols that are used to create secure VPN allow the creation of VPN that have authentication but no encryption. Although such a network is more secure than a standard network with no authentication, it is not a VPN because there is no privacy.

The security properties of the VPN must be agreed to by all parties in the VPN. Secure VPN has one or more tunnels, and each tunnel has two endpoints. Business and VPN user of the two endpoints of each tunnel must be able to agree on the security properties of the tunnel. No one outside the VPN can affect the security properties of the VPN. It must be impossible for an attacker to change the security properties of any part of a VPN, such as to weaken the encryption or to affect which encryption keys are used.

No one other than the trusted VPN provider can affect the creation or modification of a path in the VPN. The entire value of the trusted VPN is that business, partner, and staff can trust that the provider to provision and control the VPN. Therefore, no one outside the realm of trust can change any part of the VPN. Note that some VPN span more than one provider; in this case, VPN user trusts the group of providers as if they were a single provider. No one other than the trusted VPN provider can change data, inject data, or delete data on a path in the VPN. A trusted VPN is more than just a set of paths: it is also the data that flows along those paths. Although the paths are typically shared among many customers of a provider, the path itself must be specific to the VPN and no one other than trusted provider can affect the data on that path. Such a change by an outside party would affect the characteristics of the path itself, such as the amount of traffic measured on the path.

Companies who use trusted VPN do so because they want to know that their data is moving over a set of paths that has specified properties and is controlled by one ISP or a trusted confederation of ISPs. This allows the customer to use their own private IP addressing schemes, and possibly to handle their own routing. The customer trusts that the paths will be

maintained according to an agreement and that people whom the customer does not trust (such as an attacker) cannot either change the paths of any part of the VPN or insert traffic on the VPN. Note that it is usually impossible for a customer to know the paths used by trusted VPN, or even to validate that a trusted VPN is in place; they must trust their provider completely.

The routing and addressing used in a trusted VPN must be established before the VPN is created. The user must know what is expected of the VPN user, and what is expected of the service provider, so that they can plan for maintaining the network that they are purchasing.

7.3 FURTHER RESEARCH

At the conceptual level, this study focused on the contribution of information security technology and competitive advantage knowledge by business and IT professionals to their organizations with their perception of use. Further research needs to be done in the area of information security selection for implementation and deployment computer network security that are owned by corporations. This can include customers, suppliers, and partnerships that may connect to organization and headquarters networks. The further study will provide management and security professionals a basis for making decisions related to enterprise security. It provides information security vendors insight into feature requirements of the information security market, and provides academic researchers interested in security, a more focused approach on various dimensions of security devices and software's from the behavioral perspective. The expertise of IT professionals in their own domain can also be included to compare the relative contribution of their functional and cross-functional expertise to the development of organization. Further research should also test the applicability of the instrument to industries other than insurance and to different sizes of organizations.

Evaluating information security technology is controversial and often extremely difficult. In literature review, researchers suggest qualitative and quantitative approaches for these kinds of evaluations. However, qualitative or quantitative analysis in information security technology has its pros and cons. For example quantitative security analysis supporters explain that the results of a quantitative security analysis approach are substantially based on independent objective processes and metrics and they can be expressed in a management-specific language. On the other hand, opponents argue that calculations can be complex (assigning costs to security and benefits of countermeasures is difficult) and it

requires much preliminary work. Qualitative security analysis proponents believe that in their approach the calculations are simple, it is not necessary to quantify threat frequency, and many non-technical issues are easily accounted for. The opponents of the qualitative approach argue that this method is subjective in nature and the results depend heavily on the quality of the security management team assembled.

In this study, the researcher addressed VPN security issues that business and IT professionals may face in dealing with information systems that are at the heart of organizations. However, VPN, as information security technology, is an extensive area and under continuous and rapid development. The Researcher recommends that managers look at the current trends in technology, and Internet crime. The Researcher also recommends that companies have a clear understanding of their security and the best technologies that can serve as possible countermeasures. One of the approaches is to exam an information security management program. This program should include policies, procedures, and audits, as well as technological safeguards such as firewalls, encryption algorithms, authentication devices, intrusion detection systems, and network security management tools.

Even if an enterprise is able to secure an information system from its operational improvements, the question of competitive advantage via information security technology remains. One approach to assessing the implications for competitive advantage is to identify information security technology applied for strategic reasons and examine its impact on sustained performance and competitive advantage. In contrast, an event study finds that the stock market reacts favorably to announcements that firms are using strategic information security systems. Moreover, in subsequent years those enterprises tend to be more productive and more profitable than their industry rivals. There is also evidence that firms making investments in strategic information security systems achieve sustainability via their established technology base. Another approach is to assess the attributes of information security and their ability to confer competitive advantage concludes that only managerial business and IT skills confer a competitive advantage.

7.4 SUMMARY

In this research, the main reason that enterprises use secure VPN is so that they can transmit sensitive information over networking and the Internet without needing to worry about who might see it. Everything that goes over a secure VPN is encrypted to such a level that even if someone captured a copy of the traffic, they could not read the traffic even if they used hundreds of millions of dollars worth of computers. Further, using a secure VPN allows the

organisation to know that an attacker cannot alter the contents of their transmissions, such as by changing the value of financial transactions. Secure VPN is particularly valuable for remote access where a user is connected to the Internet at a location not controlled by the network administrator.

What this points out is that VPN awareness is something that enterprises will need to know, and providers will need to communicate. The simple truth is that most enterprise traffic will be carried on VPN by the end of the decade, whether the user chooses this or the provider converges into it. Only by understanding VPN and their implications can either provider or consumer is sure the changeover will be successful for all.

Based on findings from this study, one important way for an IT person to be heard is for him/her to devote the time necessary to develop shared IT knowledge, the most influential construct in the research model. The most important direct predictor of information security technology in this study was a high level of communication between business and IT professional as user perspective. However, one cannot mandate meaningful communication between individuals. An IT person needs to understand the leverage points of the industry, the history and current issues of the business units, and to learn to apply common sense in the application of technology to business problems. This change in view would help focus their attention on those technologies and ideas that could produce the most benefit, rather than those that offer the most technical promise. In this research, organizations will begin to employ extensive criteria that allow them to examine and evaluate the costs associated with security technology projects, and to make go or no-go decisions on the basis of that data. Vendors should anticipate increasing levels of scrutiny, and work on empirical means to convey evidence of value.

Security is perhaps the single most important operational issue facing organizations in today's IT driven business environment. Whether organization are operating domestically or engaged in outsourcing or off-shoring activities, they must develop and adhere to very strict security measures to protect mission critical data, confidential organization data and customer sensitive information. As the trend continues toward more internetworks that rely on electronic communication, organizations must develop measures to safeguard data integrity; protect customer information to prevent identity theft; motivate employees to perform effectively from remote locations; and manage information security technology costs and new developments in order to maintain efficient operations and gain competitive edge in the marketplace.

PUBLICATIONS

CONFERENCE PROCEEDING

Cusack, B. & Sirisukha, S. (2006). Evaulating Seamless Information Systems Security. *New Zealand Information Security Forum (NZISF)*, Auckland, New Zealand.

Sirisukha, S. (2005). Business and IT Professionals Perspective of Information Systems Security: An Evaluation and Analytical Process. *Proceedings of Beijing International Conference on Applied Business Research (BICABR), Beijing, China*.

Kotykhov, M. & Sirisukha, S. (2004). Information Systems Security: A Model for VPN Performance Evaluation. *Proceedings of the Americas Conference on Information Systems (AMCIS) 2004, New York, USA.*

Sirisukha, S. (2004). Evaluation of Intrusion Detection System Security by Using a Hierarchy of Determinant Attributes, *Proceeding of the 15th Australasian Conference on Information Systems (ACIS), Tasmania, Australia*.

Kotykhov, M. & Sirisukha, S. (2004). The role of information security variable in customer's adoption of the Internet banking. *Proceeding of the Academy of Business and Administrative Sciences (ABAS) 2004, Bratislava, Slovak Republic.*

Kotykhov, M. & Sirisukha, S. (2004). The information system security perceptions in customer's adoption of the electronic commerce. *Proceedings of the 17th National Advisory Committee on Computing Qualification (NACCQ), Christchurch, New Zealand.*

Kotykhov, M. & Sirisukha, S. (2004). Using a Hierarchy of Determinant Attributes for Evaluation of Information Security Systems: the Case of Intrusion Detection System (IDS), *Proceeding of World Scientific and Engineering Academy and Society (WSEAS), Rio de Janeiro, Brazil.*

Cusack, B., & Sirisukha, S. (2003). Integrative Approaches to Securing eBusiness Networks. *Proceedings of the 14th Australasian Conference on Information Systems (ACIS), Perth, Western Australia.*

Sirisukha, S. (2003). The Advantages of a Virtual Private Network for Computer Security. *Proceedings of the 16th National Advisory Committee on Computing Qualification (NACCQ), Palmerston North, New Zealand.*

Sirisukha, S. (2003). Building More Secure and Effective Information Systems in Organizations with Implementing Intrusion Detection. *Proceedings of the 7th Annual Waikato Management School Student Research Conference, Hamilton, New Zealand.*

Sirisukha, S. (2003). Multicast Routing Over Computer Network: Secure Performance Designs. *Proceedings of the Doctoral Consortium, The 14th Australasian Conference on Information Systems (ACIS), Perth, Western Australia.*

Sirisukha, S. (2003). The Reflections of 1st year PhD. *Proceedings of the National Advisory Committee on Computing Qualification (NACCQ), Post Graduate Symposium, Palmerston North, New Zealand.*

CONFERENCE PRESENTATIONS

Cusack, B. & Sirisukha, S. (2006). Evaulating Seamless Information Systems Security. New Zealand Information Security Forum (NZISF), Auckland, New Zealand.

Sirisukha, S. (2005). Business and IT Professionals Perspective of Information Systems Security: An Evaluation and Analytical Process. Proceedings of Beijing International Conference on Applied Business Research, Beijing, China.

Sirisukha, S. (2004). Evaluation of Intrusion Detection System Security by Using a Hierarchy of Determinant Attributes, Proceeding of the 15th Australasian Conference on Information Systems (ACIS), December 1-3, 2004, Tasmania, Australia.

Sirisukha, S. (2004). Using a Hierarchy Process to Build the Information Security Base. Proceeding of the 2004 IT Governance International Conference, November 15-16, 2004, Auckland, New Zealand.

Kotykhov, M. & Sirisukha, S. (2004). Information Systems Security: A Model for VPN Performance Evaluation. Proceeding of the Americas Conference on Information Systems (AMCIS) 2004, August 5-8, 2004, New York, USA.

Cusack, B., & Sirisukha, S. (2003). Integrative Approaches to Securing eBusiness Networks. Proceedings of the 14th Australasian Conference on Information Systems (ACIS), November 26-28, 2003, Perth, Western Australia.

Sirisukha, S. (2003). Multicast Routing Over Computer Network: Secure Performance Designs. Proceedings of the Doctoral Consortium, The 14th Australasian Conference on Information Systems (ACIS), November 26-28, 2003, Perth, Western Australia.

Sirisukha, S. (2003). The Advantages of a Virtual Private Network for Computer Security. Proceedings of the National Advisory Committee on Computing Qualification (NACCQ) 16th, July 6-9, 2003, Palmerston North, New Zealand.

Sirisukha, S. (2003). Building More Secure and Effective Information Systems in Organizations with Implementing Intrusion Detection. Proceedings of the 7th Annual Waikato Management School Student Research Conference, March 19, 2003, Hamilton, New Zealand.

REFERENCES

Abu-Musa, A. A. (2002a). Security of computerized accounting information systems: A theoretical framework. *Journal of American Academy of Business*, Cambridge, 2(1), 150.

Abu-Musa, A. A. (2002b). Security of computerized accounting information systems: An integrated evaluation approach. *Journal of American Academy of Business*, Cambridge, 2(1), 141.

Ackerman, M. S., Pipek, V., & Wulf, V. (2003). *Sharing expertise : beyond knowledge management*. Cambridge, Mass.: MIT Press.

Ackoff, R. L. (1999). Re-creating the corporation: a design of organizations for the 21st century. New York ; Oxford: Oxford University Press.

Agarwal, R., & Ferratt, T. W. (2002). Enduring practices for managing IT professionals. Association for Computing Machinery. *Communications of the ACM,* 45(9), 73.

Ali, H. A. (2001). A new model for monitoring intrusion based on Petri Nets. *Information Management & Computer Security,* 9(4), 175.

Al-Khayatt, S., Shaikh, S. A., Akhgar, B., & Siddiqi, J. (2002). A study of encrypted, tunneling models in virtual private networks. Paper presented at the Information Technology: Coding and Computing, 2002.

Alter, S. (2001). Management information systems. Electronic commerce. Publisher: Upper Saddle River, NJ: Prentice Hall.

Alter, S. (2002). Information systems: foundation of e-business, Publisher: Upper Saddle River, NJ: Prentice Hall.

Alter, S. (2002). Three critical checkpoints the collaboration triangle: a tool for improving it-business communication. *CIO insight*. New York,1(9), 1.

Alvarez-Hamelin, J. I., & Fraigniaud, P. (2003). M/spl lambda/T: a multicast protocol with QoS support. Paper presented at the Computer Communications and Networks, 2003. ICCCN 2003. Proceedings. The 12th International Conference on.

Amaratunga, D., Baldry, D., & Sarshar, M. (2001). Process improvement through performance measurement: The balanced scorecard methodology. *Work Study*, 50(4/5), 179.

An, B., & Papavassiliou, S. (2001). A mobility-based hybrid multicast routing in mobile ad-hoc wireless networks. Paper presented at the Military Communications Conference,

2001. MILCOM 2001. Communications for Network-Centric Operations: Creating the Information Force. IEEE.

Anderson, J. E., & Schwager, P. H. (2002). Security in the information systems curriculum: Identification & status of relevant issues. *The Journal of Computer Information Systems*, 42(3), 16.

Andrews, D., Preece, J., & Turoff, M. (2001). A Conceptual Framework for Demographic Groups Resistant to Online Community Interaction. Paper presented at the Presented at the HICSS 2001 Conference, Honolulu, HI.

Andrews, K. R. (1980). The Concept of Corporate Strategy. Boston, MA: RD Irwin.

Ansoff, H. I. (1984). Implanting Strategic Management. London: Prentice Hall.

Anthony, R. N. (1965). Planning and Control Systems, a Framework for Analysis. Boston Mass.: Harvard Business School Press.

Antonopoulou, H., Bogonikolos, N., Giotopoulos, K., Likothanassis, S., Tsakalidis, A., & Vassiliadis, B. (2001). A service oriented standardised system for virtual private networks. Paper presented at the Computer Systems and Applications, ACS/IEEE International Conference on. 2001.

Applegate, L. M., Austin, R. D., & McFarlan, F. W. (2003). Corporate information strategy and management : text and cases (6th ed.). Boston: McGraw-Hill Irwin.

Aqun, Z., Yuan, Y., Yi, J., & Guanqun, G. (2000). Research on tunneling techniques in virtual private networks. Paper presented at the Communication Technology Proceedings, 2000. WCC - ICCT 2000. International Conference on.

Avgerou, C. (2002). Information systems and global diversity. Oxford, New York: Oxford University Press.

Avresky, D. R., Shurbanov, V., & Horst, R. (1998). The effect of the router arbitration policy on the scalability of ServerNet topologies. *Microprocessors and Microsystems*, 21(9), 545-561.

Baek, S.-J., Jeong, M.-S., Park, J.-T., & Chung, T.-M. (2000). Policy-based hybrid management architecture for IP-based VPN. Paper presented at the Network Operations and Management Symposium, 2000. NOMS 2000. 2000 IEEE/IFIP.

Ballardie, A. J., Francis, P., & Crowcroft, J. (1993). Core Based Trees (CBT). Paper presented at the Proc. ACM SIGCOMM '93, San Francisco, CA.

Baltatu, M., Lioy, A., Maino, F., & Mazzocchi, D. (2000). Security issues in control, management and routing protocols. *Computer Networks*, 34(6), 881-894.

Bandyopadhyay, K., Mykytyn, P. P., & Mykytyn, K. (1999). A framework for integrated risk management in information technology. *Management Decision*, 37(5), 437.

Barbarosoglu, G., & Pinhas, D. (1995). Capital rationing in the pubic sector using the analytic hierarchy process. *The Engineering Economist*, 40(4), 315-341.

Bartunek, J. M., & Seo, M.-G. (2002). Qualitative research can add new meanings to quantitative research. *Journal of Organizational Behavior*, 23(2), 237.

Baskerville, R. L., & Portougal, V. (2003). A possibility theory framework for security evaluation in national infrastructure protection. *Journal of Database Management*, 14(2), 1.

Bassett, G. (1998). Designs on routing. *Timber and Wood Products*, 386(6304), 25-26.

Beauprez, J. (2002). Survey Shows Low Rates of Consumer Trust in E-Commerce, News Web Sites. *Knight Ridder Tribune Business News*, 1.

Belleflamme, P. (2001). Oligopolistic Competition, IT Use for Product Differentiation and the Productivity Paradox. *International Journal of Industrial Organization*, 19(12), 227-248.

Benantar, M. (2001). The Internet public key infrastructure. *IBM Systems Journal*, 40(3), 648.

Benbasat, I., & Weber, R. (1996). Research Commentary: Rethinking Diversity in Information Systems Research. *Information Systems Research*, 7(4), 389-399.

Berman, O., Drezner, Z., & Wesolowsky, G. O. (2000). Routing and location on a network with hazardous threats. *The Journal of the Operational Research Society*, 51(9), 1093.

Bharadwaj, A. S. (2000). A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation. *MIS Quarterly*, 24(1), 169-196.

Bhutta, K. S., & Hug, F. (2002). Supplier selection process: a comparison of the total cost of ownership and the analytic hierarchy process approaches. *Supply Chain Management: An International Journal*, 7(3), 126-135.

Binbasioglu, M., & Winston, E. (2004). Systems Thinking for Identifying Unintended Consequences of It: Packaged Software Implementation in Small Businesses. *The Journal of Computer Information Systems*, 45(1), 86.

Birnbaum, M. H. (2000). SurveyWiz and FactorWiz: JavaScript Web pages that make HTML forms for research on the Internet. *Behavior research methods, instruments and computers*, 32(2), 339-346.

Birnbaum, M. H. (2004). Human research and data collection via the internet. *Annual Review of Psychology*, 55, 803.

Black, S. E., & Lynch, L. M. (2001). How to compete: the impact of workplace practices and information technology on productivity. *Review of Economics and Statistics*, 83(3), 434-445.

Black, U. D. (2000). Internet architecture: an introduction to IP protocols. Upper Saddle River, N.J.: Prentice Hall.

Bondarouk, T., & Sikkel, K. (2005). Explaining it implementation through group learning. *Information Resources Management Journal*, 18(1), 42.

Bontis, N., & Fitz-enz, J. (2002). Intellectual capital ROI: A causal map of human capital antecedents and consequents. *Journal of Intellectual Capital*, 3(3), 223.

Botha, R. A., & Eloff, J. H. P. (2001). A framework for access control in workflow systems. *Information Management & Computer Security*, 9(2/3), 126.

Boudreau, M.-C., Gefen, D., & Straub, D. W. (2001). Validation in information systems research: A state-of-the-art assessment. *MIS Quarterly*, 25(1), 1.

Bouras, C., Ganos, P., & Karaliotas, A. (2003). The deployment of IPv6 in an IPv4 world and transition strategies. *Internet Research*, 13(2), 86.

Box, W., & Sterling, K. (2001). Enabling the User: The VPN in Context. *Information Security Technical Report*, 6(1), 65-76.

Brandyberry, A. A. (2003). Determinants of adoption for organizational innovations approaching saturation. *European Journal of Innovation Management*, 6(3), 150.

Braun, T., Guenter, M., & Khalil, I. (2001). Management of quality of service enabled VPNs. Communications Magazine, *IEEE*, 39(5), 90-98.

Brendon, C. F. (2002). In ecommerce, customer trust is no longer an option: It is the requirement for success. *Quality Congress*. ASQ's Annual Quality Congress Proceedings, 355.

Broadhead, S. (2000). Tunnel vision provides safe links. *Computer Weekly*, 74, 76.

Brooks, W. J., Warren, M. J., & Hutchinson, W. (2002). A security evaluation criteria. *Logistics Information Management*, 15(5/6), 377.

Brynjolfsson, E. (1993). The productivity paradox of information technology. Association for Computing Machinery. *Communications of the ACM*, 36(12), 67.

Brynjolfsson, E., & Hitt, L. (1993). Is information systems spending productive? Paper presented at the Proceedings of the International Conference in Information Systems, Orlando.

Brynjolfsson, E., & Hitt, L. (2000). Beyond Computation: Information Technology, Organizational Transformation and Business Performance. *Journal of Economic Perspective*, 14(4), 23-48.

Brynjolfsson, E., & Hitt, L. M. (1998). Beyond the productivity paradox. Association for Computing Machinery. *Communications of the ACM*, 41(8), 49.

Brynjolfsson, E., Hitt, L., & Yang, S. (2002). Intangible Assets: Computers and Organizational Capital. *Brookings Papers on Economic Activity*, 1, 137-181.

Burnham, D. P. (1999). Achieving prosperity: Technology, growth, productivity and culture change. *Vital Speeches of the Day*, 65(15), 465.

Buyukozkan, G. (2004). An organizational information network for corporate responsiveness and enhanced performance. *Journal of Manufacturing Technology Management*, 15(1), 57.

Cabrera, J. B. D., Lewis, L., Qin, X., Lee, W., & Mehra, R. K. (2002). Proactive intrusion detection and distributed denial of service attacks--a case study in security management. *Journal of Network and Systems Management*, 10(2), 225.

Calhoun, K. J., & Lederer, A. L. (1990). From strategic business planning to strategic information systems planning: the missing Link. *Information Technology Management*, 1(1), 1-6.

Caloyannides, M. (2003). Privacy vs. information technology. *Security & Privacy Magazine, IEEE,* 1(1), 100-103.

Camp, L. J. (2004). Identity, authentication, and identifiers in digital government. Paper presented at the Technology and Society, 2003. Crime Prevention, Security and Design. Proceedings. 2003 International Symposium on.

Canada, J. R., & Sullivan, W. G. (1996). Capital Investment Analysis for Engineering and Management. Upper Saddle River, NJ: Prentice-Hall.

Caromel, D., & Vayssiere, J. (2003). A security framework for reflective Java applications. *Software-Practice and Experience*, 33(9), 821-846.

Casper, S. (2000). Institutional adaptiveness, technology policy, and the diffusion of new business models: The case of German biotechnology. *Organization Studies*, 21(5), 887.

Casson, M. (2000). Information and organization : a new perspective on the theory of the firm. Oxford: Oxford University Press.

Chakrabarti, A., Striegel, A., & Manimaran, G. (2002). A case for tree evolution in QoS multicasting. Paper presented at the Quality of Service, 2002. Tenth IEEE International Workshop on.

Chan, Y. E., & Huff, S. L. (1992). The development of instruments to access information systems and company strategy and performance. *Working Paper*, University of Western Ontario, 92-06.

Chen, L., & Singh, G. (2002). Enhancing multicast communication to support protocol design. Paper presented at the Computer Communications and Networks, 2002. Proceedings. Eleventh International Conference on.

Chen, S., Nahrstedt, K., & Shavitt, Y. (2000). A QoS-aware multicast routing protocol. Paper presented at the INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE.

Cheng, E. W. L., & Li, H. (2001). Analytic hierarchy process: an approach to determine measures for business performance. *Measuring Business Excellence*, 5(3), 30-36.

Cheng, T. H., & Shen, Y. (1997). Nonuniform traffic analysis on a class of self-routing networks. IEE Proceedings. *Communications*, 144(3), 143-149.

Chesla, A. (2004). Information Security: A Defensive Battle. *Information Systems Security*, 12(6), 24.

Cheung, K. H., & Misic, J. (2002). On virtual private networks security design issues. *Computer Networks*, 38(2), 165-179.

Chichester, West Sussex, England ; Hoboken, NJ: J. Wiley.

Chinn, S. S. (2001). The technology paradox. *Industrial Management*, 43(2), 25.

Choi, T., Chung, H., Kim, C., & Jeong, T. (2003). Design and implementation of an information model for integrated configuration and performance management of MPLS-TE/VPN/QoS. Paper presented at the Integrated Network Management, 2003. IFIP/IEEE Eighth International Symposium on.

Chowdhury, S., & Chan, J. (2005). Decision Support Systems - An IT and Industrial Perspective. *Journal of American Academy of Business, Cambridge*, 6(2), 172.

Chuvakin, A. (2004). Security Event Analysis through Correlation. *Information Systems Security*, 13(2), 13.

Claver, E., Gonzalez, R., & Llopis, J. (1993). An analysis of research in information systems (1981-1997). *Information and Management*, 24, 121-133.

Claxton, T. (2001). Improving Internet collaboration. Petroleum Review, 55(659), 32-33.

Clip, P. (1998). IIOP: the next HTTP? *Byte*, 23(1), 47-48.

Cohen, N. (2000). IT credential to help CPAs make business sense out of technology. *Information Technology Management*, 3(2), 1-6.

Collins, C., & Clark., M. (2003) Enhancing SMTEs' business performance through the Internet and e-learning platforms. *Education & Training*, 45 (8/9), 483-485.

Comer, D., Prasad, N., & Prasad, A. (2002). Internetworking with TCP/IP. Vol. 1, Principles, protocols, and architecture WLAN systems and wireless IP for next generation communications (4th ed.). Upper Saddle River, N.J: Prentice Hall ; Prentice-Hall International Artech House.

Conorich, D. G. (2004). Monitoring Intrusion Detection Systems: From Data to Knowledge. *Information Systems Security*, 13(2), 19.

Corradi, A., & Stefanelli, C. (1996). A deadlock prevention strategy for adaptive routing systems. *Microprocessors and Microsystems*, 20(2), 97-103.

Cortese, G., Fiutem, R., Cremonese, P., D'antonio, S., Esposito, M., Romano, S. P., et al. (2003). Cadenus: creation and deployment of end-user services in premium IP networks. *Communications Magazine, IEEE*, 41(1), 54-60.

Cotter, D., & Tatham, M. C. (1997). `Dead reckoning'-a primitive and efficient self-routing protocol for ultrafast mesh networks. IEE Proceedings. *Communications*, 144(3), 135-142.

Couper, M. P. (2000). Web-based surveys: A Review of Issues and Approaches. *Public Opinion Quarterly* 64.

Creswell, J. W. (2003). Research design: qualitative, quantitative, and mixed method approaches (2nd ed.). Thousand Oaks, Calif.: Sage Publications.

Cui, W., & Bassiouni, M. A. (2003). Virtual private network bandwidth management with traffic prediction. *Computer Networks*, 42(6), 765-778.

Cusack, B., & Sirisukha, S. (2003). Integrative Approaches to Securing Ebusiness Networks. Paper presented at the Proceedings of the 14th Australasian Conference on Information Systems (ACIS), Scarborough Beach, Western Australia.

Dabbous, W. S. (1997). High-performance protocol architecture. *Computer Networks and ISDN Systems*, 29(7), 735-744.

Dai, J., Pung, H. K., & Angchuan, T. (2002). A multicast routing protocol supporting multiple QoS constraints. Paper presented at the Networks, 2002. ICON 2002. 10th IEEE International Conference on.

Damianides, M. (2004). Sarbanes-Oxley and IT governance: New guidance on IT control and compliance. *Edpacs*, 31(10), 1.

Davies, J., & Lee, T. (1999). Widows 2000 TCP/IP Protocols and Services Technical Reference: Microsoft Press.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User Acceptance Of Computer Technology: A Comparison Of Two. *Management Science*, 35(8), 982.

Davis, L., & Williams, G. (1994). Evaluating and selecting simulation software using the analytic hierarchy process. *Integrated Manufacturing Systems*, 5(1), 23-32.

De Clercq, J., & Paridaens, O. (2002). Scalability implications of virtual private networks. Communications Magazine, *IEEE*, 40(5), 151-157.

DeFillippi, R. J. (2002). Organizational models for collaboration in the new economy. *HR. Human Resource Planning*, 25(4), 7.

Dennis, A. (2002). Networking in the Internet age: New York : Wiley.

Devaraj, S., & Kohli, R. (2002). The IT payoff : measuring the business value of information technology investments. New York: Financial Times Prentice Hall.

Devaraj, S., & Kohli, R. (2003). Performance Impacts of Information Technology: Is Actual Usage the Missing Link. *Management Science*, 49(3), 273-289.

Dey, P. K. (2001). Decision support system for risk management: case study. *Management Decision*, 39(8), 634-649.

Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. Association for Computing Machinery. *Communications of the ACM*, 43(7), 125.

Doll, W. J., & Torkzadeh, G. (1987). The relationship of MIS steering committees to the size of firm and formalization of MIS planning. *Communications of the ACM*, 30(11).

Dunham, K. (2004). EICAR Test File Security Considerations. *Information Systems Security*, 12(6), 7.

Dunsky, G. (2003). An intelligent approach to making tunnels safe. *Traffic Engineering & Control*, 44(3), 98-99.

Earl, M. J. (1989). Management Strategic for Information Technologies. London: Prentice.

El-Sayed, M., & Jaffe, J. (2002). A view of telecommunications network evolution. Communications Magazine, *IEEE*, 40(12), 74-81.

Evans, S., Heinbuch, D., Kyule, E., Piorkowski, J., & Wallner, J. (2004). Risk-based Systems Security Engineering: Stopping Attacks with Intention. *Security & Privacy Magazine, IEEE*, 2(6), 59-62.

Fedorowicz, J., & Ulric, J. (1998). Adoption and Usage Patterns of COBIT: Result from survey of COBIT purchasers. *Information Systems Audit & Control*, 6, 45-51.

Feng, G., Mao, K., & Pissinoul, N. (2002). Efficient implementations of bounded shortest multicast algorithm. Paper presented at the Computer Communications and Networks, 2002. Proceedings. Eleventh International Conference on.

Fenner, G. H., & Renn, R. W. (2004). Technology-assisted supplemental work: Construct definition and a research framework. *Human Resource Management*, 43(2-3), 179.

Ferraris, M., Frixione, P., & Squarcia, S. (2001). Network oriented radiological and medical archive. *Computer Physics Communications*, 140(1-2), 226-232.

Fichman, R. G. (2001). The role of aggregation in the measurement of IT-related organizational innovation. *MIS Quarterly*, 25(4), 427.

Filali, F., & Dabbous, W. (2002). A simple and scalable fair bandwidth sharing mechanism for multicast flows. Paper presented at the Network Protocols, 2002. Proceedings. 10th IEEE International Conference on.

Fitzgerald, E. P. (1993). Success measures for information systems strategic planning. *Strategic Information Systems*, 2(4), 335-350.

FitzGerald, J. (2002). Business data communications and networking: New York : John Wiley.

FitzGerald, J., Panko, R. R., & Harle, D. (2000). Business data communications and networking Data communication and networks : an engineering approach: New York : John Wiley Upper Saddle River New York ; Chichester : Wiley.

Flammini, M., Leeuwen, J. v., & Marchetti-Spaccamela, A. (1998). The complexity of interval routing on random graphs. *Computer Journal*, 41(1), 16-25.

Foley, S. N., & Dumigan, R. (2001). Are handheld viruses a significant threat? Association for Computing Machinery. *Communications of the ACM*, 44(1), 105.

Forcht, K. A. & Ayers, R. (2000). Security-related concerns with geographic information systems and geographic mapping. *Information Management & Computer Security*, 8(5), 218.

Forouzan, B. A., & Fegan, S. C. (2001). Data communications and networking: Boston: McGraw-Hill.

Forouzan, B. A., Coombs, C. A., & Fegan, S. C. (2001). Data communications and networking (2nd ed.). Boston: McGraw-Hill.

Foss, N. J. (1997). Resources, firms, and strategies : a reader in the resource-based perspective. Oxford ; New York: Oxford University Press.

Fowler, F. J. (2002). Survey research methods (3rd ed. Vol. v. 1). Thousand Oaks, Calif.: Sage Publications.

Frei, F. X., & Harker, P. T. (1999). Measuring aggregate process performance using AHP. *European Journal of Operational Research*, 116, 436-442.

Gable, G. (1994). Integrating Case Study and Survey Research Methods: An Example in Information Systems. *European Journal of Information Systems*, 3(2), 112-126.

Gallegos, F. (2004). Information technology control and audit (2nd ed.). Boca Raton, Fla.: Auerbach Publications.

Galliers, R. D. (1987). Information System Planning in Britain and Australia in the mid-1980s: Key Success Factor., Ph.D. Dissertation, University of London, London.

Galliers, R. D., & Leidner, D. E. (2003). Strategic information management : challenges and strategies in managing information systems (3rd ed.): Butterworth-Heinemann.

Galliers, R. D., Merali, Y., & Spearing, L. (1994). Coping with information technology? How British executives perceive the key issues in the mid-1990's. Information *Technology*, 9(4), 223-238.

Gann, R. (2000). A connection shared. Personal Computer World, 23(10), 323-324.

Gary J Mann, G. J., & Mahmood, M. A. (2000) Special issue: Impacts of information technology investment on organizational performance. *Journal of Management Information Systems*, 16(4), 3.

Gasco, J. L., Llopis, J., & Gonzalez, M. R. (2004). The use of information technology in training human resources: An e-learning case study. *Journal of European Industrial Training*, 28(5), 370.

Gates, M. S., & Ryan, S. D. (2004). Inclusion of social subsystem issues in IT investment decisions: An empirical assessment Information *Resources Management Journal*,17(1), 12

Gaynor, D. (2002). IT governance. *Accountancy Ireland*, 34(4), 28.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Inexperience and experience with online stores: The importance of TAM and trust. *IEEE Transactions on Engineering Management*, 50(3), 307.

Geiselmann, W., Meier, W., & Steinwandt, R. (2003). An attack on the isomorphisms of polynomials problem with one secret. International *Journal of Information Security,* 2(1), 59.

Gelinas, U. J., Sutton, S. G., & Fedorowicz, J. (2004). Business processes and information technology. Mason, Ohio: Thomson / South-Western.

Gengler, B. (1999). Check point outlines VPN strategy. *Network Security*, 1999(6), 6-7.

Gentry, P. B. (2001). What is a VPN? *Information Security Technical Report*, 6(1), 15-22.

Gershman, C. (2002). Tunneling solves IP traffic snarls. *Electronic Engineering Times,* (1243), 70.

Gershman, C. (2002). Tunneling solves IP traffic snarls. *Electronic Engineering Times* (1243), 70.

Ghanem, S. I. (2000). Doing Quantitative Research in the Social Sciences: An Integrated Approach to Research Design, Measurement and Statistics. *International Journal of Public Opinion Research*, 12(1), 95.

Gibson, J. L. (2003). Organizations : behavior, structure, processes (11th ed.). Boston, Mass.: McGraw-Hill/Irwin.

Giese, X. (2002). Cisco networking academy program : fundamentals of web design companion guide: Indianapolis.

Griffis, S. E., Goldsby, T. J., & Cooper, M. (2003). WEB-BASED AND MAIL SURVEYS: A COMPARISON OF RESPONSE, DATA, AND COST. *Journal of Business Logistics,* 24(2), 237.

Grosse, E., & N, L. Y. (2003). Network processors applied to IPv4/IPv6 transition. *IEEE Network,* 17(4), 35.

Grover S Kearns, G. S., & Albert L Lederer, A., L. (2003) A Resource-Based View of Strategic IT Alignment: How Knowledge Sharing Creates Competitive Advantage *Decision Sciences.* 34 (1), 29.

Guldentops, E., & De Haes, S. (2002). COBIT 3rd Edition Usage Survey: Growing Acceptance of COBIT. *Information Systems Control*, 6, 25-31.

Gunes, S., Yilmaz, N., & Allahverdi, N. (2001). A multicast routing algorithm based on parallel branching method for faulty hypercubes. Paper presented at the EUROCON'2001, Trends in Communications, International Conference on.

Gyires, T. (2003). Software agents architecture for controlling long-range dependent network traffic. *Mathematical and Computer Modelling*, 38(7-9), 839-848.

Hain, T. (2003). Advanced software paves path to IPv6. *Communication Systems Design*, 9(5), 10.

Hanks, S., Farinacci, D., & Traina, P. (1994). Generic Routing Encapsulation (GRE). *RFC* 1701.

Hanks, S., Li, T., Farinacci, D., & Traina, P. (1994). Generic Routing Encapsulation over IPv4 networks. *RFC* 1702.

Harding, A. (2003). SSL Virtual Private Networks. *Computers & Security*, 22(5), 416-420.

Hardjono, T., & Cain, B. (1999). A secure group membership verification protocol for IP multicast. Paper presented at the Computers and Communications, 1999. Proceedings. IEEE International Symposium on.

Harrington, H. J. (1991). Business process improvement : the breakthrough strategy for total quality, productivity and competitiveness. New York: McGraw-Hill.

Harrington, H. J., Esseling, E. K. C., & Nimwegen, H. v. (1997). Business process improvement workbook : documentation, analysis, design, and management of business process improvement. New York: McGraw-Hill.

Hatch, M. J. (1997). Organization theory : modern, symbolic, and postmodern perspectives: Oxford : Oxford University Press.

Haughwout, A. F. (2000). The paradox of infrastructure investment. *The Brookings Review*, 18(3), 40.

Haworth, D., & Pietron, L. (2006). SARBANES-OXLEY: ACHIEVING COMPLIANCE BY STARTING WITH ISO 17799. *Information Systems Management*, 23(1), 73.

Hazari, S. (2002). Reenineering an information security course for business management focus. *Journal of Information Systems Education*, 13(3), 197.

He, J., Blight, D., & Chujo, T. (2000). A unified architecture for virtual private networking. Paper presented at the Communication Technology Proceedings, 2000. WCC - ICCT 2000.

Held, G., Forouzan, B. A., & Fegan, S. C. (2002). Quality of service in a Cisco networking environment Data communications and networking: Chichester: Wiley Boston: McGraw-Hill.

Henderson, J. C., & Venkatraman, H. (1991) Aligning Business and Information Technology Domains: Strategic Planning in Hospitals. *Hospital & Health Services Administration.* 37(1), 71.

Henderson, J. C., & Venkatraman, H. (1999) Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal,* 38, (2/3), 472.

Henderson, J., & Sifonis, J. (1988). Understanding the value of IS planning:understanding consistency, Validity and IS market. *MIS Quarterly*, 12(2), 187-200.

Henderson, J., & Venkatraman, N. (1992). Strategic alignment: a model for organizational transformation through information technology. In Transforming Organizaions, Oxford University Press, New York.

Henderson, J.C, & Venkatraman, N.(1993) Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal*. 32(1), 4.

Henry, P. A. (2004). Protocol and Application Awareness: A New Trend or an Established Tradition? *Information Systems Security*, 12(6), 33.

Heuring, V. P., Jordan, H. F., & Murdocca, M. (2003). Computer systems design and architecture (2nd ed.). Upper Saddle River, NJ: Pearson/Prentice Hall.

Hicks, M., Keromytis, A. D., & Smith, J. M. (2003). A secure PLAN. Systems, Man and Cybernetics, Part C, *IEEE Transactions on*, 33(3), 413-426.

Hitt, L., & Brynjolfsson, E. (1996). Productivity, Business Profitability, and Consumer Surplus: Three Different Measures of Information Technology Value. *MIS Quarterly*, 20(2), 121-142.

Hitt, L., Wu, D. J., & Zhou, X. (2002). Investment in Enterprise Resource Planning: Business Impact and Productivity Measures. *Journal of Management Information Systems*, 19(1), 71-98.

Holland, P. J., Hecker, R., & Steen, J. (2002). Human resource strategies and organisational structures for managing gold-collar workers. *Journal of European Industrial Training*, 26(2-4), 72.

Hong, K.-S., Chi, Y.-P., Chao, L. R., & Tang, J.-H. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, 11(5), 243.

Hopstaken, B. A. A., & Kranendonk, A. (1985). Informatieplanning: een eenvoudige aanpakk voor een complex problem. *Informatie*, 27(11), 988-998.

Horovitz, J. (1984). New perspectives on strategic management. *Business Strategy*, 4(3), 19-33.

Householder, A., Houle, K., & Dougherty, C. (2002). Computer attack trends challenge Internet security. *Computer*, 35(4), 5.

Huang, K.-M., & Chang, C.-J. (2003). A fast multicast IP-routing lookup scheme. Communications Letters, *IEEE,* 7(3), 133-135.

III, E. E. L., & Mohrman, S. A. (2003). HR as a strategic partner: What does it take to make it happen? HR. *Human Resource Planning*, 26(3), 15.

Im, Y., & Choi, Y. (1998). A distributed multicast routing algorithm for delay-sensitive applications. Paper presented at the Parallel and Distributed Systems, 1998. Proceedings., 1998 International Conference on.

Imielinski, T., & Navas, J. C. (1999). GPS-based geographic addressing, routing, and resource discovery. Association for Computing Machinery. *Communications of the ACM,* 42(4), 86.

Inayatullah, S., & Leggett, S. (2002). Transforming communication : technology, sustainability, and future generations. Westport, Conn.: Praeger.

Inge, J., & McLean, I. (2000). The fundamentals of systems & security maintenance Windows 2000 TCP/IP black book. Washington, D.C.

Institute, I. G. (2001). Board briefing on IT governance, on-line available at www.itg.org.

IV, J. W. L. (2000). Why IT governance is a top management issue. *The Journal of Corporate Accounting & Finance,* 11(5), 33.

IV, J. W. L. (2001). An IT assurance framework for the future. Ohio CPA Journal, 60(1), 19.

Iyengar, J. V. (2004). A discussion of current and potential issues relating information security for internet communications. *Competitiveness Review*, 14(1/2), 90.

Jackson, M., & Twaddle, G. (1997). Business process implementation: building workflow systems. Harlow, Essex.: Addison-Wesley.

Jarvenpaa, S. L., & Ives, B. (1993). Organizing for global competition: the fit of information technology. *Decision Sciences*, 24(3), 547-580.

Jeong, M., Qiao, C., & Vandenhoute, M. (2002). Distributed shared multicast tree construction protocols for tree-shared multicasting in OBS networks. Paper presented at the Computer Communications and Networks, 2002. Proceedings. Eleventh International Conference on.

John, A., Sugla, B., Krishnan, H., Park, E., Raghu, A., Sequiera, R., et al. (2003). An architecture for provisioning IP services in an operations support system. Paper presented at the Integrated Network Management, 2003. IFIP/IEEE Eighth International Symposium on.

Johnson, R. R. (2004). Persuasive Technology: Using Computers to Change What We Think and Do. *Journal of Business and Technical Communication*, 18(2), 251.

Johnson, T. (1997). Time to take control: the impact of change on corporate computer systems. Boston: Butterworth-Heinemann.

Johnston, D. L. (1998). Open networks, electronic commerce and the global information infrastructure. *Computer Standards & Interfaces*, 20(2-3), 95-99.

Jones, M. T. (2002). TCP\IP application layer protocols for embedded systems (1st ed.). Hingham, Mass.: Charles River Media.Journal of Accountancy. *New York*, 190(1), 95.

Kaczmarczyk, S., & Murtough, J. (2002). Measuring the performance of innovative workplaces. *Journal of Facilities Management*, 1(2), 163.

Kagaris, D. (1997). A routing algorithm for row-based FPGAs. *Microprocessors and Microsystems,* 20(7), 401-407.

Kalakota, D. R., & Konsynski, D. B. (2000). The Rise of Neo-Intermediation: The Transformation of the Brokerage Industry. *Information Systems Frontiers*, 2(1), 115.

Kalatoa, F. & Robinson, D. C. (2001). The influence of information technologies on theology. *Theological Studies*, 62 (2), 366 -373.

Kaplan, R. S., & Norton, D. P. (1999). The balanced scorecard: translating strategy into action. Boston, Mass.: Harvard Business School Press.

Keen, P. G. W., & Scott Morton, M. S. (1978). Decision Support Systems: An Organizational Perspective. Reading, MA: Addison-Wesley.

Keenan, R. (2003). Group to roll switch fabric and IPv6 benchmarks. *Electronic Engineering Times,* (1279), 24.

Kenning, M. J. (2001). Security Management Standard -- ISO 17799/BS 7799. *BT Technology Journal,* 19(3), 132.

Kesh, S., Ramanujan, S., & Nerur, S. (2002). A framework for analyzing e-commerce security. *Information Management & Computer Security*, 10(4), 149.

Keskin, H. & Zehir, C. (2003). A field research on the effects of MIS on organizational restructuring. *Journal of American Academy of Business*, 3(1). 270.

Kijkanjanarat, T., & Chao, H. J. (1999). Fast IP routing lookups for high performance routers. *Computer Communications*, 22(15-16), 1415-1422.

Kindred, D., & Sterne, D. (2001). Dynamic VPN communities: implementation and experience. Paper presented at the DARPA Information Survivability Conference & Exposition II, 2001. DISCEX '01. Proceedings.

King, A., & Hunt, R. (2000). Protocols and architecture for managing TCP/IP network infrastructures. Computer Communications, 23(16), 1558-1572.

Knahl, M., Hofmann, H. D., & Phippen, A. (1999). A distributed component framework for integrated network and systems management. *Information Management & Computer Security*, 7(5), 254.

Knight, G. (1998). Trading Securities on the Web. Paper presented at the eCommerce - Trading But Not As We Know It (Ref. No. 1998/460), IEE Colloquium on.

Kodialam, M., Lakshman, T. V., & Sengupta, S. (2003). Online multicast routing with bandwidth guarantees: a new approach using multicast network flow. *Networking, IEEE/ACM Transactions on*, 11(4), 676-686.

Kolokotronis, N., Margaritis, C., Papadopoulou, P., Kanellis, P., & Martakos, D. (2002). An integrated approach for securing electronic transactions over the Web. *Benchmarking*, 9(2), 166.

Korac-Kakabadse, N., & Kakabadse, A. (2001). IS/IT governance: Need for an integrated model. *Corporate Governance*, 1(4), 9.

Kraemer, K. L., Dedrick, J., & Yamashiro, S. (2000). Refining and Extending the Business Model with Information Technology: Dell Computer Corporation. *The Information Society* . 16(1), 5-21.

Krigline, A. G., & Rakich, J. S. (1987). Productivity Improvement through Better Problem Solving by Supervisors. *National Productivity Review (1986-1998)*, 7(1), 61.

Kruh, L. (2002). Certified information systems security professionals. *Cryptologia*, 26(2), 145.

Kuo, J., & Burns, C. M. (2000). A work domain analysis for virtual private networks. Paper presented at the Systems, Man, and Cybernetics, 2000 IEEE International Conference on.

Labib, A., Williams, G., & O'Connor, R. (1997). An intelligent maintenance model (system): an application of AHP and a fuzzy logic rule based controller. Paper presented at the Proceedings of the First European Conference on Intelligent Management Systems in Operations, University of Salford.

Labib, A., Williams, G., & O'Connor, R. (1997). Deriving a maintenances strategy through the application of a multiple criteria decision making technology. Paper presented at the Proceedings of the 12th International Conference in MCDM, Springer Verlag, New York, Berlin, Heidelberg.

Labonte, C., & Srinivas, S. (2000). Group management strategies for secure multicasting on active virtual private networks. Paper presented at the Local Computer Networks, 2000. LCN 2000. Proceedings. 25th Annual IEEE Conference on.

Lambrinoudakis, C. (2000). Smart card technology for deploying a secure information management framework. *Information Management & Computer Security*, 8(4), 173.

Landau, S. (2000). Designing cryptography for the new century. Association for Computing Machinery. *Communications of the ACM*, 43(5), 115.

Landwehr, C. E. (2001). Computer security. International *Journal of Information Security*, 1(1), 3.

Lanz, J., & Tie, R. (2004). Advise Businesses on External IT Resources. *Journal of Accountancy*, 197(6), 55.

Lawson, R., Stratton, W., & Hatch, T. (2003). The Importance of True Balance. *CMA Management,* 77(8), 36.

Lawson, S. (2002). IPv6 enters the real world. InfoWorld, 24(7), 35.

Lawson, S. (2003). NetScreen among firms adding IPv6 to firewalls. *Network World*, 20(28), 19.

Lederer, A. L., & Mendelow, A. (1986). Issues in information systems planning. *Information Management,* 10(5), 245-254.

Lederer, A. L., & Mendelow, A. (1989). The coordination of information systems plans with business plans. *Management Information Systems*, 6(2), 5-19.

Lee, B., & Menon, N. M. (2000) Information technology value through different normative lenses *Journal of Management Information Systems.* 16 (4), 99.

Lee, D., Lin, A. W., Hutton, T., Akiyama, T., Shinji, S., Lin, F.-P., et al. (2003). Global Telescience featuring IPv6 at iGrid2002. *Future Generation Computer Systems,* 19(6), 1031-1039.

Lee, H., Kwak, W., & Han, I. (1995). Developing a business performance evaluation system: an analytic hierarchical model. *The Engineering Economist*, 40(4), 343-357.

Lee, T. E., & Jones, R. (2001). What might go wrong with LAN design and implementation? *The Journal of Computer Information Systems*, 42(2), 51.

Lee, T. H., Wood, R. C., & Shiba, S. j. (1999). Integrated management systems : a practical approach to transforming organizations. New York ; Chichester: Wiley.

Lewis, B. R., & Byrd, T. A. (2003). Development of a measure for the information technology infrastructure construct. *European Journal of Information Systems*, 12(2), 93.

Li, C., Harms, G, & Bai. L. (2003) Organizational factors influencing the quality of the IS/IT strategic planning process. *Industrial Management & Data Systems*, 103, (8/9), 622-631.

Lin, H.-C., & Lai, S.-C. (2000). A simple and effective core placement method for the core based tree multicast routing architecture. Paper presented at the Performance, Computing, and Communications Conference, 2000. IPCCC '00. Conference Proceeding of the IEEE International.

Logan, J. R. (2002). Evolution not revolution : aligning technology with corporate strategy to increase market value. New York: McGraw-Hill.

London. Nonnecke, B., & Preece, J. (2000). Lurker demographics: counting the silent. Paper presented at the Human Factors in Computing Systems, The Hague, Holland.

Long, L. E., & Long, N. (2004). Computers : information technology in perspective (11th ed.). Upper Saddle River, N.J.: Pearson/Prentice Hall.

Loveman, G. (1988). An assessment of the productivity impact of information technologies. In MIT management in the nineties (pp. 88). Massachussetts Institute of Technology, Cambridge.

Lucas, H. C. (1999). Information technology and the productivity paradox : assessing the value of investing in IT. New York: Oxford University Press.

Luftman, J., & Brier, T. (1999). Achieving and sustaining business-IT alignment. California *Management Review*, 42(1), 109.

Luftman, J., & D Sledgianowski, D. (2005). IT-Business Strategic Alignment Maturity: A Case Study. *Journal of Cases on Information Technology*. 7 (2), 102.

Lund, C., Phillips, S., & Reingold, N. (1999). Paging against a Distribution and IP Networking. *Journal of Computer and System Sciences*, 58(1), 222-231.

Mackay, M., Edwards, C., Dunmore, M., Chown, T., & Carvalho, G. (2003). A scenario-based review of IPv6 transition tools. *Internet Computing, IEEE*, 7(3), 27-35.

Mahmood, M. A., & Mann, G. J. (2000). Special issue: Impacts of information technology investment on organizational performance. *Journal of Management Information Systems,* 16(4), 3.

Main, A. (2004). Application Security: Building in Security during the Development Stage. *Information Systems Security,* 13(2), 31.

Maiwald, E. (2002). Securing business information : strategies to protect the enterprise and its network Network security : a beginner's guide. Hillsboro, Or. New York: Intel Press ; Addison-Wesley Osborne/McGraw-Hill.

Mamaghani, F. (2002). Evaluation and selection of an antivirus and content filtering software. *Information Management & Computer Security*, 10(1), 28.

Mambretti, J., & Schmidt, A. (1999). Next generation Internet : creating advanced networks and services. New York: Wiley.

Mansfield, N. (2003). Practical TCP/IP : designing, using, and troubleshooting TCP/IP networks on Linux and Windows. Boston: Addison-Wesley.

Maresca, R., D'Arienzo, M., Esposito, M., Romano, S. P., & Ventre, G. (2002). An active network approach to virtual private networks. Paper presented at the Computers and Communications, 2002. Proceedings. ISCC 2002. Seventh International Symposium on.

Mark Pullen, J. (2000). The Network Workbench: network simulation software for academic investigation of Internet concepts. *Computer Networks*, 32(3), 365-378.

Markus, M. L. (1994). Electronic Mail as the Medium of Managerial Choice. *Organization Science*, 5(4), 502-527.

Markus, M. L., & Robey, D. (2004). Why Stuff Happens: Explaining the Unintended Consequences of Using Information Technology. The Past and Future of Information Systems, K.

Marsan, C. D. (2001a). ISP group at vortex of IPv6 transition. *Network World*, 18(30), 25.

Marsan, C. D. (2001b). Mobile security flaw delivers yet another blow to IPv6. *Network World*, 18(14), 1.

Martin, N., Gregor, S., & Hart, D. (2005). THE SOCIAL DIMENSION OF BUSINESS AND IS/IT ALIGNMENT: CASE STUDIES OF SIX PUBLIC-SECTOR ORGANISATIONS. *Australian Accounting Review*, 15(3), 28.

McAdams, A. (2004). SECURITY AND RISK MANAGEMENT: A FUNDAMENTAL BUSINESS ISSUE. *Information Management Journal*, 38(4), 36.

McCoy, S., & Marks, P. V., Jr. (2001). Using electronic surveys to collect data: experiences from the field. Paper presented at the Paper presented at the AMCIS conference. . Boston, MA.

McDermott, P. (2000). Security in IP Networks. *Network Security*, 2000(12), 7-9.

McFarlan, F. W. (1984). Information technology changes the way you compete. Harvard *Business Review*, 62(1), 98-103.

McGregor, J. P., & Lee, R. B. (2000). Performance impact of data compression on virtual private network transactions. Paper presented at the Local Computer Networks, 2000. LCN 2000. Proceedings. 25th Annual IEEE Conference on.

McKenney, J. L., Copeland, D. C., & Mason, R. O. (1995). Waves of change : business evolution through information technology. Boston, Mass.: Harvard Business School Press.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on Intentions to transact with a web site: a trust building model. *Journal of Strategic Information Systems*, 11(3/4), 297–323.

McLoone, M., & McCanny, J. V. (2002). A single-chip IPSEC cryptographic processor. Paper presented at the Signal Processing Systems, 2002. (SIPS '02). IEEE Workshop on.

Mercuri, R. (2003). Standards Insecurity. *Association for Computing Machinery. Communications of the ACM,* 46(12), 21.

Mingers, J. (2001). Combining IS Research Methods: Towards a Pluralist Methodology. *Information Systems Research*, 12(3), 240-259.

Mintzberg, H. (1980). Opening up the definition of strategy. In The Concept of Corporate Strategy, RD Irwin, Boston, MA.

Mintzberg, H., & Quinn, J. B. (1996). The strategy process : concepts, contexts, cases (3rd ed.). Upper Saddle River, N.J.: Prentice Hall.

Mohamed, S. (1996). Benchmarking and improving construction productivity. *Benchmarking for Quality Management & Technology,* 3(3), 50.

Montgomery, C. A., & Porter, M. E. (1991). Strategy : seeking and securing competitive advantage (12th ed.). Boston, Mass.: Harvard Business School Press.

Moreton, R., & Chester, M. (1996). Transforming the business : the IT contribution. New York: McGraw-Hill Publ.

Motyckova, L., & Jennings, E. (1999). A clustering structure for reliable multicasting. Paper presented at the Computer Communications and Networks, 1999. Proceedings. Eight International Conference on.

Moy, J. (1994). Multicast Extensions to OSPF (MOSPF) ,. Proteon Inc., RFC 1584.

Mukhopadhyay, T., Kekre, S., & Kalathur, S. (1995). Business value of information technology: A study of electronic data interchange. *MIS Quarterly*, 19(2), 137.

Nambisan, S., Agarwal, R., & Tanniru, M. (1999). Organizational mechanisms for enhancing user innovation in information technology. *MIS Quarterly*, 23(3), 365.

Nelson, K. M., Nadkarni, S., Narayanan, V. K., & Ghods, M. (2000). Understanding software operations support expertise: A revealed causal mapping approach. *MIS Quarterly*, 24(3), 475.

Nicolle, L. (2001). Has IPv6 risen to the challenge? Computer Weekly, 44-45.

Niederman, F., Brancheau, J., & Wetherbe, J. (1991). Information systems management issues in the 1990s. *MIS Quarterly*, 15(4), 474-500.

Nonnecke, B. (2000). Lurkers in email-based discussion lists. South Bank University,.

Noor, A. K. (1997). New computing systems and future high-performance computing environment and their impact on structural analysis and design. *Computers & Structures*, 64(1-4), 1-30.

Ohata, T., Fukui, T., Ishii, M., Furukawa, Y., Nakatani, T., Matsushita, T., et al. (2001). Secure network for beamline control. Nuclear Instruments and Methods in Physics

Research Section A: Accelerators, Spectrometers, *Detectors and Associated Equipment*, 467-468(Part 1), 825-828.

Orlikowski, W. J., & Iacono, C. S. (2001). Desperately Seeking the 'IT' in IT Research--A Call to Theorizing the IT Artifact. *Information Systems Research*, 12(2), 121-134.

Orlikowski, W., & Baroudi, J. J. (1991). Studying Information Technology in Organizations: Research Approaches and Assumptions. *Information Systems Research*, 2(1), 1-28.

Owen, K., Mundy, R., Guild, W., & Guild, R. (2001). Creating and sustaining the high performance organization. *Managing Service Quality*, 11(1), 10.

Palmer, C. C. (2001). Ethical hacking. *IBM Systems Journal*, 40(3), 769.

Palshaugen, O., Shotter, J., Gustavsen, B., & rn. (1998). The end of organization theory? : language as a tool in action research and organizational development: Amsterdam ; Philadelphia : John Benjamins Pub.

Pan, Y., Yu, Z., & Wang, L. (2003). A genetic algorithm for the overlay multicast routing problem. Paper presented at the Computer Networks and Mobile Computing, 2003. ICCNMC 2003. 2003 International Conference on.

Pandey, S., Somani, A., & Tyagi, A. (2003). Intermediate processing protocol for processing within IP-routed networks. *Microprocessors and Microsystems*, 27(5-6), 285-295.

Panko, R. R. (2000). Business data communications and networking (3rd ed.). Upper Saddle River, NJ: Prentice Hall.

Paolo, A. M., Bonamino, G. A., Gibson, D., Patridge, T., & Kallail, K. (2000). Response rate comparisons of email and mail distributed student evaluations. *Teaching and Learning in Medicine*, 12(2), 81-84.

Parker, M. M., Benson, R. J., & Trainor, H. E. (1988). Information economics : linking business performance to information technology. Englewood Cliffs, N.J.: Prentice Hall.

Patton, S., Smith, B., Doss, D., & Yurcik, W. (2000a). A layered framework strategy for deploying high assurance VPNs. Paper presented at the High Assurance Systems Engineering, 2000, Fifth IEEE International Symposim on. HASE 2000.

Patton, S., Smith, B., Doss, D., & Yurcik, W. (2000b). A virtual private network deployment framework. Paper presented at the Local Computer Networks, 2000. LCN 2000. Proceedings. 25th Annual IEEE Conference on.

Pena, C. J. C., & Evans, J. (2000). Performance evaluation of software virtual private networks (VPN). Paper presented at the Local Computer Networks, 2000. LCN 2000. Proceedings. 25th Annual IEEE Conference on.

Pereira, R. E. (2002). An adopter-centered approach to understanding adoption of innovations. *European Journal of Innovation Management*, 5(1), 40.

Pettigrew, A. M. (1987). Context and action in the transformation of the firm. *Management Studies*, 24(6), 649-670.

Pinsonneault, A., & Rivard, S. (1998). Information technology and the nature of managerial work: From the productivity paradox to the Icarus paradox? *MIS Quarterly*, 22(3), 287.

Porter, M. E. (1998). Competitive strategy : techniques for analyzing industries and competitors : with a new introduction (1st Free Press ed.). New York: Free Press.

Porter, M. E. (2001). Competition and antitrust: Toward a productivity-based approach to evaluating mergers and joint ventures. *Antitrust Bulletin*, 46(4), 919.

Porter, M. E., & Stern, S. (2001). Innovation: Location Matters. *MIT Sloan Management Review*, 42(4), 28.

Premkumar, G. (1992). An empirical Study of IS planning characteristics among industries. *Omega*, 20(5), 611-629.

Pusateri, T. (1998). Distance Vector Multicast Routing Protocol. *IETF Draft update to RFC* 1075, 3(6).

Pyburn, P. (1983). Linking the MIS plan with corporate strategy: an exploratory study. *MIS* Quarterly, 7(2), 1-14.

Qu, W., & Srinivas, S. (2002). IPSec-based secure wireless virtual private network. Paper presented at the MILCOM 2002. Proceedings.

Quinn, L. R., & Brill, A. E. (2002). Risky business. *Journal of Accountancy*, 193(6), 65.

Rangone, A. (1996). An analytical hierarchy process framework for comparing the overall performance of manufacturing departments. *International Journal of Operation & Production Managment*, 16(8), 104-119.

Ranky, P. G. (2000). Modular fieldbus designs and applications. *Assembly Automation*, 20(1), 40-45.

Ravichandran, T., & Rai, A. (2000). Quality management in systems development: An organizational system perspective. *MIS Quarterly*, 24(3), 381.

Ravindran, K., & Liu, X. (2002). Integration of flow and QOS control in multicast routing. Paper presented at the Computer Communications and Networks, 2002. Proceedings. Eleventh International Conference on.

Raz, D., & Shavitt, Y. (2000). Active networks for efficient distributed network management. *Communications Magazine, IEEE*, 38(3), 138-143.

Redlich, J.-P., Suzuki, M., & Weinstein, S. (1999). Virtual networks in the Internet. Paper presented at the Open Architectures and Network Programming Proceedings, 1999. OPENARCH '99. 1999 IEEE Second Conference on.

Renkema, T. J. W. (2000). The IT value quest : how to capture the business value of IT-based infrastructure. New York: John Wiley & Sons.

Rhee, M. Y. (2003). Internet security : cryptographic principles, algorithms, and protocols.

Richard, C., & Chung, C.-J. (2000). A mobile multicast protocol with error control for IP networks. Paper presented at the Global Telecommunications Conference, 2000. GLOBECOM '00. IEEE.

Richard, T., & Ballard, M. (1995). Business information : technologies and strategies. Cheltenham, Glos.: Stanley Thornes.

Rickard, J. T., & Torre, N. G. (1999). Information systems for optimal transaction *Implementation. Journal of Management Information Systems*, 16(2), 47.

Ritchey, R., O'Berry, B., & Noel, S. (2002). Representing TCP/IP connectivity for topological analysis of network security. Paper presented at the Computer Security Applications Conference, 2002. Proceedings. 18th Annual.

Robey, D. R. (1996). Diversity in Information Systems Research: Threat, Promise, and Responsibility. *Information Systems Research*, 7(4), 400-408.

Rosenbaum, G., Lau, W., & Jha, S. (2003). An analysis of virtual private network solutions. Paper presented at the Local Computer Networks, 2003. LCN '03. Proceedings. 28th Annual IEEE International Conference on.

Ross, J., Goodhue, D., & Beath, C. (1996). Develop Long-Term Competitiveness through IT Assets. *Sloan Management Review*, 31-42.

Ross, K. W., & Tittel, E. (2001). Computer networking : a top-down approach featuring the Internet Computer networking: Reading London : McGraw-Hill.

Ross, K. W., Tittel, E., Forouzan, B. A., & Fegan, S. C. (2003). Computer networking : a top-down approach featuring the Internet Computer networking Data communications and networking: Reading London : McGraw-Hill Boston : McGraw-Hill.

Rossi, P. H., Freeman, H. E., & Lipsey, M. W. (1999). Evaluation : a systematic approach (6th ed.). Thousand Oaks, Calif.: Sage Publications.

Rowley, J. E., & Farrow, J. (2000). Organizing knowledge : an introduction to managing access to information (3rd ed.). Aldershot, Hampshire, England ; Burlington, Vt.: Gower.

Saaty, T. L. (1983). Priority Setting in Complex Problems. *IEEE Transactions on Engineering Management, EM30*(3), 140.

Saaty, T. L. (1986). Scaling the Membership Function. *European Journal of Operational Research,* 25(3), 320.

Saaty, T. L. (1994). How to make a decision: The analytic hierarchy process. *Interfaces*, 24(6), 19.

Sabherwal, R., & Becerra-Fernandez, I. (2003). An Empirical Study of the Effect of Knowledge Management Processes at Individual, Group, and Organizational Levels. *Decision Sciences*, 34(2), 225.

Sarathy, R., & Muralidhar, K. (2002). The security of confidential numerical data in databases. *Information Systems Research*, 13(4), 389.

Sarkar, S., & Tassiulas, L. (2002). A framework for routing and congestion control for multicast information flows. Information Theory, *IEEE Transactions on*, 48(10), 2690-2708.

Scambray, J., McClure, S., & Kurtz, G. (2001). Hacking exposed : network security secrets & solutions (2nd ed.). Berkeley, Calif.: Osborne/McGraw-Hill.

Schafer, G. (2001). Placement of Intelligence Within Networks to Provide Corporate VPN Services. *Information Security Technical Report*, 6(1), 77-94.

Schwenk, C. R. (1988). The Essence of Strategic Decision Making. Lexington, MA: D.C. Heath.

Scottsdale, AZ: American Hotel and Lodging Association Coriolis Group Books.

Severance, D. G., & Passino, J. (2002). Making I/T work : an executive's guide to implementing information technology systems (1st ed.). San Francisco: Jossey-Bass.

Shank, R., Niblock, E. G., & Sandalls, W. T. (1973). Balance creativity and practicality in formal planning. *Harvard Business Review*, 51(1), 87-95.

Shin, N. (2003). Creating business value with information technology : challenges and solutions. Hershey, Pa.: Idea Group Pub.

Shirey, R. (2000). Internet Security Glossary: RFC 2828.

Sichel, D. E. (1997). The computer revolution : an economic perspective. Washington, D.C.: Brookings Institution Press.

Simco, G. (2001). Performance evaluation and the Internet 2 performance initiative. *The Internet and Higher Education*, 4(2), 125-136.

Simon, H. (2003). Software patches said to be insufficient against computer attack. *Aviation Week's Homeland Security & Defense*, 2(35), 3.

Siponen, M. (2002). Towards maturity of information security maturity criteria: Six lessons learned from software maturity criteria. *Information Management & Computer Security*, 10(5), 210.

Slay, J. (2003). IS security, trust and culture: A theoretical framework for managing IS security in multicultural settings. *Campus - Wide Information Systems*, 20(3), 98.

Smith, H. L., Jr, W. I. B., & Piland, N. F. (2000). Does information technology make a difference in healthcare organization performance? *A multiyear study. Hospital Topics*, 78(2), 13.

Solms, R. v. (1997). Driving safely on the information superhighway. *Information Management & Computer Security*, 5(1), 20.

Sprague, R. H., & Carlson, E. D. (1982). Building Effective Decision Support Systems. New York: Prentice Hall.

Stacey, R. D. (1996). Strategic management and organisational dynamics (2nd ed.). London: Pitman.

Stallings, W. (2000a). Computer organization and architecture: designing for performance: Upper Saddle River.

Stallings, W. (2000b). Network security essentials: applications and standards. Upper Saddle River, NJ: Prentice Hall.

Stallings, W. (2004). Data and computer communications (7th ed.). Upper Saddle River, N.J.: Pearson/Prentice Hall.

Stanton, J. M., & Coovert, M. D. (2004). Guest editors' note: Turbulent waters: The intersection of information technology and human resources. Human *Resource Management*, 43(2-3), 121.

Stephen Ackroyd, S. (2002). Collectivities in social and organizational theory. *Management Research News*. 25, (8-10), 12.

Sterman, J. D., Repenning, N. P., & Kofman, F. (1997). Unanticipated side effects of successful quality programs: Exploring a paradox of organizational improvement. *Management Science*, 43(4), 503.

Subramanian, R., & Ostrowski, M. (2002). A hardware/software architecture for 3G baseband processing. *Electronic Engineering*, 74(905), 58-60.

Tallon, P. P., Kraemer, K. L., & Gurbaxani, V. (2000). Executives' perceptions of the business value of information technology: A process-oriented approach. *Journal of Management Information Systems*, 16(4), 145.

Tanenbaum, A. S. (1996). Computer Network. Upper Saddle River, New Jersey: Printice-Hall.

Tanenbaum, A. S. (2002). Computer networks (4th ed.). Upper Saddle River, N.J. ; London: Prentice Hall.

Taylor, H. (2000). Does Internet research work? Comparing online survey results with telephone survey. *International Journal of Market Research*, 42(1), 51-63.

Theeuwes, J. A. M. (1987). Informatieplanning, Kluwer, Deventer.

Trappey, A., & Ho, P.-S. (2002). Human resource assignment system for distribution centers. *Industrial Management + Data Systems*, 102(1/2), 64.

Truell, A. D. (2003). Use of internet tools for survey research. *Information Technology, Learning, and Performance Journal*, 21(1), 31.

Tsai, C.-F., Tsai, C.-W., & Wu, H.-C. (2001). A novel multimedia multicast routing approach for the internet. Paper presented at the Multimedia and Expo, 2001. ICME 2001. IEEE International Conference on.

Tsai, H.-L. (2003). Information technology and business process reengineering : new perspectives and strategies. Westport, Conn.: Praeger.

Tse, S. S. H., & Lau, F. C. M. (1998). More on the efficiency of interval routing. *Computer Journal*, 41(4), 238-242.

Tsoukas, H., & Knudsen, C. (2003). The Oxford handbook of organization theory: Oxford ; New York : Oxford University Press.

Tudor, J. K. (2000). Information security architecture Jan Killmeyer Tudor. Boca Raton, FL: Auerbach.

Tuten, T. L., Bosnnjak, M., & Brandilla, W. (2000). Banner - advertised web-based surveys. *Marketing Research*, 11(4), 17-21.

Tyler, R. (1999). Implementing COBIT in New South Wales Heath. EDP Audit, Control and *Security Newsletter*, 27(1), 1-6.

Van Grembergen, W. (2002). Introduction to the mini track IT Governance and its Mechanisms. Paper presented at the Proceedings of the 35th Hawaii International Conference on System Sciences (HICSS).

Van Grembergen, W., & Van Bruggen, R. (2002). Measuing and improving corporate Information Technology through the balanced scorecard technique. Paper presented at the In proceeding of the European Conference on the Evaluation of Information Technology, Delft, The Netherlands.

Vargas, L. G. (1990). An overview of the analytic hierarchy process and its application. *European Journal of Operational Research*, 48, 2-8.

Venkatraman, N. (1989). The concept of fit in strategy research: toward verbal and statistical correspondence. *Academy of Management Review*, 14(3), 423-444.

Vermaas, K., & Wijngaert, L. v. d. (2005). Measuring internet behaviour: total time diary and activity diary as research methods. *JITTA : Journal of Information Technology Theory and Application*, 7(1), 121.

Wabalickis, R. N. (1987). Justification of FMS with the analytic hierarchy process. *Journal of Manufacturing Systems*, 7(3), 175-182.

Wærn, Y., & NetLibrary, I. (1998). Co-operative process management cognition and information technology. London ; Bristol, PA: Taylor & Francis.

Walshman, G., & Waema, T. (1994). Information systems strategy and implementation: a case study of a building society. *ACM Transactions on Information Systems*, 12(2), 150-173.

Wan, Z. W., Kadoch, M., & Elhakeem, A. (2003). Performance evaluation of tree-based reliable multicast. Paper presented at the Computer Communications and Networks, 2003. ICCCN 2003. Proceedings. The 12th International Conference on.

Wang, T.-Y., Wuu, L.-C., & Huang, S.-T. (2002). A scalable core migration protocol for dynamic multicast tree. Paper presented at the Parallel and Distributed Systems, 2002. Proceedings. Ninth International Conference on.

Ward, J., & Peppard, J. (2002). Strategic planning for information systems (3rd / ed.). Chichester: Wiley.

Warren, M., & Hutchinson, W. (2003). A security risk management approach for e-commerce. *Information Management & Computer Security*, 11(5), 238.

Watson, H. J., Taylor, K. P., Higgins, G., Kadlec, C., & Meeks, M. (1999). Leaders Assess the Current State of the IS Academic Discipline. *Communications of the AIS*, 2(2).

Weerakkody, V., Currie, W. L., & Ekanayake, Y. (2003). Re-engineering business processes through application service providers: Challenges, issues and complexities. *Business Process Management Journal*, 9(6), 776.

West, J. (2001). The mystery of innovation: Aligning the triangle of technology, institutions and organisation. *Australian Journal of Management*, 26, 21.

Wetteroth, D. (2001). OSI reference model for telecommunications. New York ; London: McGraw-Hill.

Whitley, R. (2000). The institutional structuring of innovation strategies: Business systems, firm types and patterns of technical change in different market economies. *Organization Studies*, 21(5), 855.

Whitmore, J. J. (2001). A method for designing secure solutions. *IBM Systems Journal*, 40(3), 747.

Wieland, K. (2002). Addressing the IPv6 issue. *Telecommunications International*, 36(5), 27.

Willcocks, L. (1994). Information Management: Evaluation of Information Systems Investments. Chapman and Hall, London.

Willcocks, L., & Graeser, V. (2000). Delivering business value from IT. Oxford: Butterworth-Heinemann.

Willcocks, L., & Graeser, V. (2000). Delivering business value from IT. Oxford: Butterworth-Heinemann.

Willcocks, L., & Lester, S. (1996). The evaluation and management of information systems investments: from feasibility to routine operations. In (1996). Investing In Information Systems: Evaluation and Management. Chapman and Hall, London.

Willcocks, L., Currie, W., & Mason, D. (1996). Informaiton Systems at Work:People Politics and Technology. Maidenhead, UK: McGraw-Hill.

Williams, M. L., & Frolick, M. N. (2001). The Evolution of EDI for Competitive Advantage: The FedEx Case. *Information Systems Management*, 18(2), 47-53.

Wilson, T. D. (1989). The implementation of IS strategies in UK companies. Information Management, 9(4), 245-258.

Witt, L. A., & Burke, L. A. (2002). Selecting high-performing information technology professionals. *Journal of End User Computing*, 14(4), 37.

Wong, W. (2002). Support IPv6 Now Or Later? *Electronic Design*, 50(17), 46.

Wool, A. (2002). Why security standards sometimes fail. *Association for Computing Machinery. Communications of the ACM*, 45(12), 144.

Wright, B. E., Manigault, L. J., & Black, T. R. (2004). Quantitative research measurement in public administration: An assessment of journal publications. *Administration & Society*, 35(6), 747.

Wright, D. (2002). Comparative evaluation of electronic payment systems. *Infor*, 40(1), 71.

Wu, C.-H., & Jan, R.-H. (2003). System integration of WAP and SMS for home network system. *Computer Networks*, 42(4), 493-502.

Xianwei, Z., Changjia, C., & Gang, Z. (2000). A genetic algorithm for multicasting routing problem. Paper presented at the Communication Technology Proceedings, 2000. WCC - ICCT 2000. International Conference on.

Yang, S. J., & Park, S. H. (2001). A dynamic service range-based multicast routing scheme using RSVP in mobile IP networks. Paper presented at the Global Telecommunications Conference, 2001. GLOBECOM '01. IEEE.

Ye, N., Giordano, J., & Feldman, J. (2001). A process control approach to cyber attack detection. *Association for Computing Machinery. Communications of the ACM*, 44(8), 76.

Yoke, C. (2002). Two years later, still sticking with IPv4. *Network World*, 19(19), 47.

Yoon, W., Lee, D., Youn, H. Y., Lee, S., & Koh, S. J. (2002). A combined group/tree approach for scalable many-to-many reliable multicast. Paper presented at the INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE.

Yoon, Y., & Im, K. S. (2005). An Evaluation System for IT Outsourcing Customer Satisfaction Using the Analytic Hierarchy Process. *Journal of Global Information Management*, 13(4), 55.

Younglove, R. W. (2001). Public key infrastructure. How it works. *Computing & Control Engineering Journal*, 12(2), 99-102.

Yuan, R., & Strayer, T. (2001). Virtual private networks : technologies and solutions. Harlow: Addison-Wesley.

Yuan, R., Scott, C., & Erwin, M. (1998). Virtual private networks: technologies and solutions Virtual private networks Creating business value with information technology : challenges and solutions Network and netplay : virtual groups on the Internet Building virtual communities : learning and change in cyberspace: Harlow : Addison-Wesley Cambridge : O'Reilly Hershey Menlo Park New York : Cambridge University Press.

Yuan, Z., Guangsheng, L., Qirong, M., Yongzhao, Z., & Yibin, H. (2003). A dynamic broadcast ring based multicast routing protocol for ad hoc networks. Paper presented at the Computer Networks and Mobile Computing, 2003. ICCNMC 2003. 2003 International Conference on.

Zagorsky, J. L. (2003). Business information : finding and using data in the digital age. Boston: McGraw-Hill.