AN INVESTIGATION INTO THE CYBERSECURITY READINESS OF THE HOSPITALS IN TONGA.

A THESIS SUBMITTED TO AUCKLAND UNIVERSITY OF TECHNOLOGY
IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF INFORMATION SECURITY AND DIGITAL FORENSICS

Supervisor
Dr. Alan. T. Litchfield.

1st May, 2024

By
Rosaviolet Kauata Holani
School of Engineering, Computer and Mathematical Sciences

Abstract

This research addressed the risks and threats to cybersecurity (CS) faced in the health industry by identifying the cultural and socio-political risk factors. The focus was based in the hospitals in Tonga, an island nation in the South Pacific. Its unique culture and socio-political norms were examined to identify the risk factors and vulnerabilities that would stand as a challenge or become a threat towards the new digital Health Information System (HIS) that has just recently rolled out in their main hospital. The process of establishing a link between systems in the main hospital on the main island and the rest of the hospitals in the outer islands is currently underway. The research method used is based on information gathered from literature reviews, reports, governmental documents, surveys, current affairs in Tonga and personal knowledge. The findings did identify multiple risk factors created by the social class and the hierarchical system in Tonga. It gave birth to privilege, factions, favouritism, and nepotism, which have been problems in Tonga for a long time.

On the other hand, the culture of gender appropriation, the traditional division of labour among men and women, has been a challenge to women moving forward in many areas traditionally dominated by men, for example, in computer technology and CS. There is a strong link between this culture and the lack of Tongan women in the tech industry and women who chose to study in the area. Most employees who are users of the new systems in Tongan hospitals are women identified as potential risks and senior employees who refused to accept new technology or bother with the required training. Other risks identified were Tonga's socio-political norm and taste for control, which was reflected in the new eGovernment plans to centralise government structure, management, and digital information under one watchful eye of the Tongan Govt. There are benefits to gain from centralised systems as well as risks in the case of cyberattacks on the one hand and accumulating too much power on the other hand that would lead to tyrannical power abuse. Tonga's diplomatic relations also reflect their cultural norm on interdependence and reliance on foreign aid, bank loans, and remittance, which has pressured Govt policies to be more in line with aid donors' objectives. It shifts our attention to China and its influence in Tonga, where China

has a reputation for CS breaches and cybercrimes.

Tonga is currently going through a digital revolution since fast broadband was brought in, mass access to smart devices and social media, the digitisation of both private and public sectors and the rollout of the eGovernment with the aim to unify all of Tonga's Govt ministries and agencies digital information under one portal. Technology has developed much faster, while the culture and tradition remain, which are incompatible and have become a challenge, creating risks compromising CS.

This research has not only exposed those risks but also stressed the importance of securing data and information held in hospitals' HIS because of their sensitivity and significance. The HIS and Information Computer Technology (ICT) systems that run hospitals must be secured to guarantee the continuation of services and caring for the vulnerable who need those services the most.

Contents

List of Tables

List of Figures

Attestation of Authorship

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.

Signature of student

Acknowledgements

I want to acknowledge a small group for their support during this journey. I thank our Heavenly Father for His guidance and strength during this challenging journey. To my son Anthony IV, thank you for your patience in allowing me to carry on and complete this research. I owe you lots for the sacrifice.
Another huge malo 'aupito goes out to several colleagues in Tonga for all the assistance, you know who you are! Your contribution helped complete this research. This research would also assist policymakers, legislators, executives, and managers in hospitals and all sectors in developing strong cybersecurity in Tonga. I would also like to acknowledge the MOH plan report for ADB showcasing Tonga's first e-Government structure and first digital HIS for the inspiration for this research.
To my supervisor, Dr.Alan Litchfield, thank you for all the mahitahi, guidance, and patience throughout this journey. Thank you for introducing me to LaTex and tutoring me through it. This is a great tool for writing and managing references in the thesis calibre. I am still amazed by the pdf view!
To everyone else who helped me in one way or another, I thank you from the bottom of my heart. 'Ofa atu and God Bless.

Dedication

I dedicate this study to my late father, Livai, my dear late mother, Luisa Va, and my late brother, Anthony Strand Snr. I wish you were all here with me on my journey. To my son Anthony IV, I hope to inspire you to chase your dreams.
To my late grandfather, Siosiua Lolohea Kaihau Holani (Papa), thank you for the discipline and guidance that weaved my foundation. You and Dad are my inspiration to carry on! I hope to fill a quarter of your shoes and the legacy you left behind.
'Ofa atu, I will always carry you all in my heart,
Rosaviolet Kauata.

Chapter 1

Introduction

1.1 Introduction

The security preparedness of Tonga's hospitals is the focus of this study. The emphasis is on the socio-political, cultural, and social risk factors as security threats to the Health Information System (HIS) and Cybersecurity (CS) in Tonga's hospitals. Identifying cultural risk is the main goal of the research. Understanding the risk can help identify mitigations for CS issues and design effective security policies. The findings of this study have implications for both the public and private sectors in Tonga and aid in creating the proper CS culture in hospitals.

This research uses interpretive methods, adhering to principles that ensure trustworthiness and avoid bias in the study and result. Research is carried out through observation of primary and secondary literary resources, video footage, experiences and knowledge of Tongan society's social culture and socio-politics.

The study finds seven risk factors that threaten HIS and information security in Tongan hospitals and are analysed in Chapter 4. Five of the risk factors are social culture factors and two socio-political factors. Section 4.4.1 relates to privilege and corruption, which indicate social stratification and social class as a risk factor. Section 4.4.2 uncover centralisation leadership and network in the new e-Government as security risk factor two. Division of labour is analysed in Section 4.4.3. Kinship, kainga (blood relations) and the tradition of Fahu privilege are analysed in Section 4.4.4 as the fourth risk factor. Section 4.4.5 is related to boundaries regarding gender appropriation and career choice. The socio-political factor of foreign influences as a security risk factor is analysed in Section 4.4.6 followed by China as a risk factor in Section 5.2.7. The remaining parts of Chapter 1 cover a brief background story on the research topic,

namely Tonga as a country in Section 1.3 and health sector as well as the current status of health care in Section 1.4.1. Section 1.2 provides the motivation for the research, Section 1.5 poses the research question, Section 1.6 details the research methodology, and Section 1.7 lays out the structure of the thesis.

1.2 Motivation

This section briefly outlines the motivation behind this research and explains what this study aims to achieve. Tonga's hospital network going digital for the first time is significant for Tonga. Tonga's embrace of digital solutions benefits social and economic development. However, it also opens the door to a new wave of CS threats and problems for Information and Communications Technology (ICT) and HIS in hospitals. This study aims to identify the cultural risks that threaten the digital networks of hospitals in Tonga. The research's conclusions improve the hospital network's security readiness. The results could also contribute to better CS legislation and effective policies that benefit not only hospitals but all public and private sectors in Tonga.

Witnessing Tonga's health sector and government go digital for the first time is significant. The question of how this new development could be sustained and preserved and the knowledge of the nature of the security risks that digital technology poses in a Tongan context motivates this study. A digital development of this magnitude is the first of its kind in the Pacific and is a pilot project that other Pacific countries will later implement. Digitalisation is a significant milestone for Tonga and the Pacific—the dawn of a new digital era that improves communication between government agencies. Despite economic and geographical barriers, this digital solution significantly improves service delivery and brings communities together.

In the digital world, great things come at a price, and cyber risk is paramount. Organisations worldwide invest significant financial resources in securing its technological systems, but the most significant weakness lies in human factors. In the case of Tonga, this study focuses on social culture and socio-political aspects to identify risk. Tonga's traditional culture is unique, and its impact on all aspects of society, regardless of social class, is significant. Social and cultural influence is reflected in government policies, religion, politics and diplomacy. There are concerns about the impact of human factors and Tongan social culture on the new HIS at Vaiola Hospital and the security and privacy of information generated and stored by the hospital. The same concern should apply equally to all public and private organisations.

This study reveals the lack of information or previous studies on cultural risks and CS implications in

the Tongan context. The study draws attention to the cultural risks. It emphasises how crucial it is for the Ministry of Health (MoH) to safeguard data, information, and intangible assets by ensuring the new HIS is well-maintained and secure. The significance of human involvement in maintaining information security is also recognised as the most significant risk factor despite solid security measures regarding the latest software and technology. Human risk factors are the most significant risk to CS, as well as security information and privacy. This draws attention to Tonga's social environment, Tongan culture and socio-political activities. Tonga is culturally unique because certain cultural traditions are considered risks to CS.

Information and privacy security is essential as new digital adoption is imposed on an environment where most users lack digital skills, knowledge or security awareness. Therefore, this study examines the social risks related to information security and privacy in a Tongan context. This study identifies the risk of traditional culture and socio-political phenomena in Tonga to the readiness of CS at the new digital HIS in hospitals.

1.3 Geography and Political Status

This section introduces Tonga as the setting for this research, with a brief description of the geographical features that host the health sector. Tonga's political status lies with the government, which owns and operates the hospitals.

Tonga is a Polynesian island nation located in the South Pacific, (Figure 1.1). Tonga comprises over 170 islands spread across six island groups: Tongatapu, Vava'u, Ha'apai, 'Eua, Niua Toputapu, and Niua Fo'ou. According to the latest census, Tonga has a population of 105,000, with 73% residing in mainland Tongatapu, 15% in Vava'u, 6% in Ha'apai, 5% in 'Eua, and 1% per cent in the Niuas area (Ministry of Health Tonga, 2019) (Table 1.1).

Tonga is the sole remaining constitutional monarchy in the Pacific region. Tonga's constitutional monarch is headed by the crown, the current King Tupou VI. The legislative, judicial, and executive branches make up the three main parts of the government system. Each government ministry is headed by a minister. In Tonga, all hospitals and health clinics throughout the country are owned and operated by the government through the MoH. It is these hospitals that are the focus of this research (Figure 1.2).

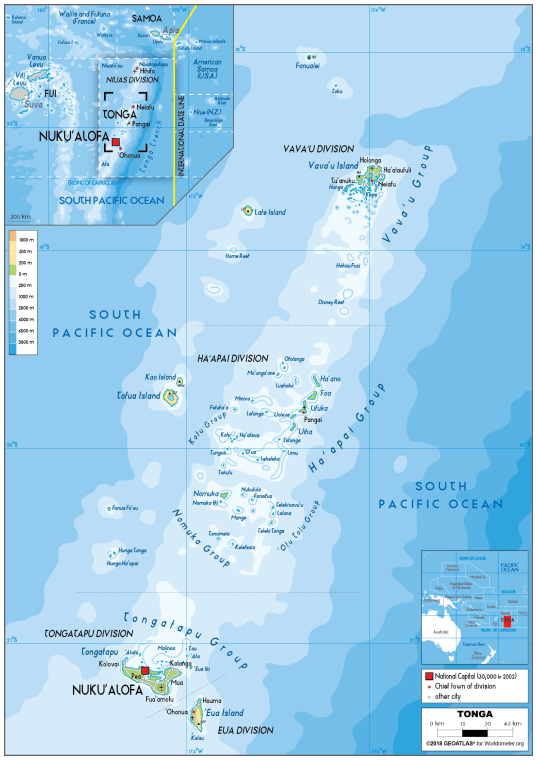

Figure 1.1: The Kingdom of Tonga (Ministry of Health Tonga, 2019)

1.4 e-Government and Digital Roll-out

This section briefly introduces digital development in the MoH as part of Tonga's e-government deployment plan. This is a turning point for Tonga's development and creates new challenges in the security of systems and data information in hospitals. One of the main threats in the Tongan context is the cultural factor. Finding these cultural risks is the primary goal of this study.

The transition from a manual, paper-based, and fragmented HIS to a centralised digital system is a growing phenomenon, and government adoption of e-government frameworks is a growing trend worldwide. This approach is being introduced into the Pacific region via Tonga and is a pilot project that will be implemented elsewhere in the Pacific. The digital health project for Tonga started in October 2019, with most components of the rollout completed in 2022 and operations and maintenance continuing until 2027 (Ministry of Health Tonga, 2019). The project's goal is to assist the Tongan Government's digital initiative. Providing beneficial services to the people of Tonga, not just in healthcare but across the public sector, will represent a significant of the achievement. The new eGovernment structure will also connect the Government as a user with businesses and the people through the Government portal. This new e-structure brings communities together through digital technology to connect people through

public services (Figure 1.2).

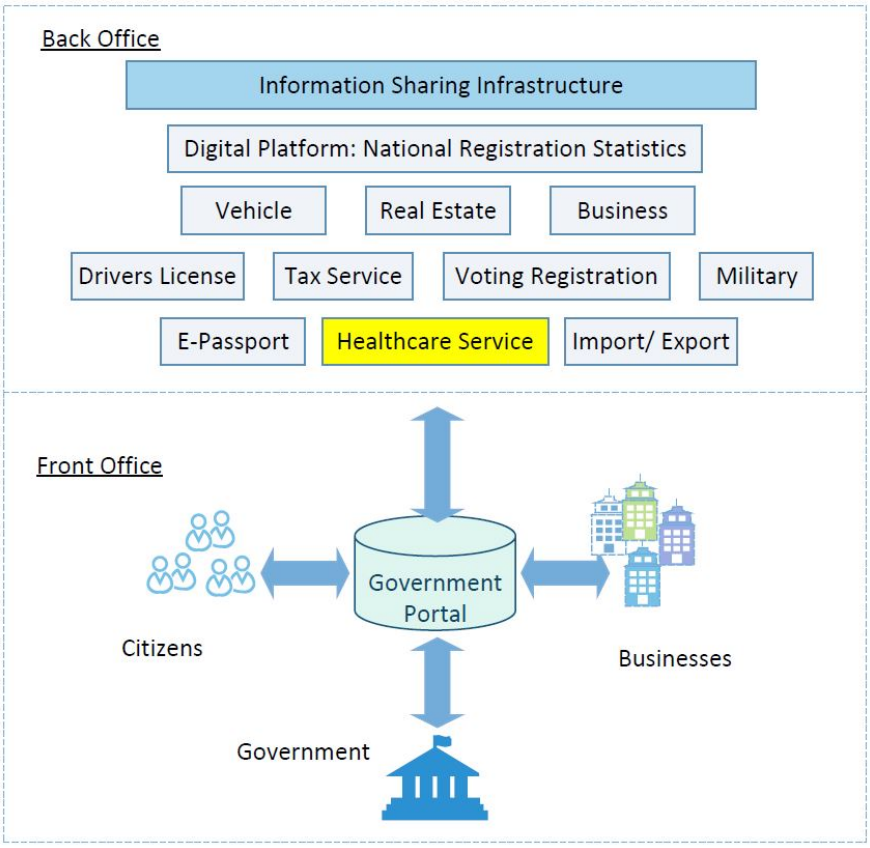

Figure 1.2: Tonga's e-Government digital framework (Ministry of Health Tonga, 2019)

1.4.1 Healthcare Delivery in Tonga

This section briefly introduces the nature of healthcare in Tonga to illustrate why a digital healthcare solution is necessary. The importance of this digital adoption to healthcare care and delivery highlights why information security is critical in hospitals.

Healthcare in Tonga is provided by private practices, hospitals, clinics, and health centres, all of which are regulated by the MoH. The Tongan Government works with organisations such as MFAT, WHO, UNFPA, ADB, UNDP, DFAT and World Bank to finance public health initiatives, whereas private practices are independently funded and managed. The MoH and donor partners are working to establish multiple clinics, health centres, and hospitals throughout Tonga, including Vaiola Hospital on Tongatapu Island (Table 1.1 and Figure 1.3).

Ministry of Health Tonga (2019) reports that Vaiola Hospital has 184 beds and serves both local residents and patients from outer islands. In 2018, the hospital treated 7,123 outpatients and 819 inpatients.

Complex cases are addressed in Vaiola Hospital, while those requiring specialised care are transferred to hospitals in New Zealand and Australia

Islands	Population	Clinics	Centers	Hospitals	Hospital Name
Tongatapu	73%	18	7	1	Vaiola
'Eua	5%	2	0	1	Niu'eiki
Ha'apai Group	6%	6	2	1	Princess Fusipala
Vava'u Group	15%	6	2	1	Prince Wellington Ngu
Niua Group	1%	2	1	1	Likamonu

Table 1.1: Tonga's population & Health facilities per Island Group

Hospitals, clinics and health centres form the interface between Tonga's healthcare system and interaction with society, and the MoH, as a Government agency, is the governing body responsible for facilitating and providing quality healthcare services to the people of Tonga. These duties are line with a framework that includes a strategic emphasis on six critical areas (Ministry of Health Tonga, 2019): Information, research, policy and planning, infrastructure, medical products and technology, leadership and governance, health workforce, service delivery, and health financing.

1.4.2 ICT and Network Infrastructure

The ICT and infrastructure scale of the Tonga hospital network is briefly described in this section. Understanding the architecture of the healthcare network is essential to controlling and reducing security threats in an efficient manner. Tonga's health network topology reflects the topography of its scattered islands as well as the culture and society. Understanding the architecture of the healthcare network is essential to controlling and reducing security threats in an efficient manner. The goal of this research is to pinpoint the cultural hazards that jeopardise hospital data storage and system security. This will aid in the creation of security solutions that are appropriate for Tonga's distinct healthcare system.

Prior to the adoption of digitalisation, the majority of hospitals in Tonga had established their own network infrastructure (Ministry of Health Tonga, 2019). Figure 1.3 present an overview of the entire MoH network. This integrates wireless access points with wired connections (CAT5/CAT6 UTP or fibre optic). There are VPN tunnels in place connecting other hospitals and health facilities to the main MoH site at Vaiola Hospital. The digital rollout expands on the current network infrastructure by establishing connections between Vaiola Hospital, the remaining clinics and health centres nationwide, and all district hospitals. Medical systems and hospital ICT can now share and communicate data in real-time like never before.

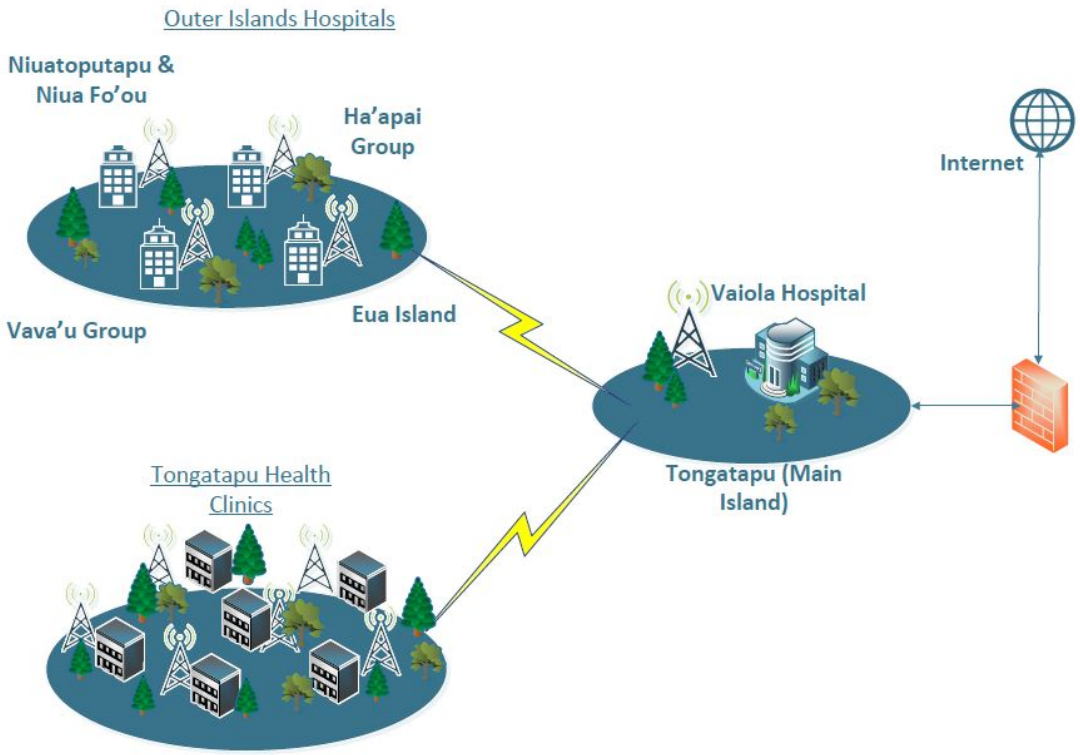

Figure 1.3: Tonga's Healthcare Overall Network (Ministry of Health Tonga, 2019)

1.5 Research Questions

The risks that human factors in CS pose on a social, cultural, and political level are highlighted in the literature review that is presented in Chapter 2. There have not been any comparable studies done in Tonga, that could apply to other Pacific nations with comparable cultures. In order to identify the vulnerabilities and risks that pose a risk to the security and privacy of information in the new HIS and ICT in hospitals in Tonga, this research fills the gap by looking at Tongan culture and socio-political attitudes. The study makes an effort to respond to the following query:

> What are the cultural risk factors in the Tongan cultural context that identify as security threats to the CS readiness of digital HIS in Tonga?

This research aims to uncover Tonga's unique cultural and socio-political risk factors that may directly impact security readiness in Tonga's hospital networks. It is recognised that social culture as a by product of human factors pose a direct risk to cyber and information security (Figure 1.4). No matter how advanced or secure a technology is, the human factor is the weakest link or Trojan horse that can determine the success or failure of a healthcare security mechanism.

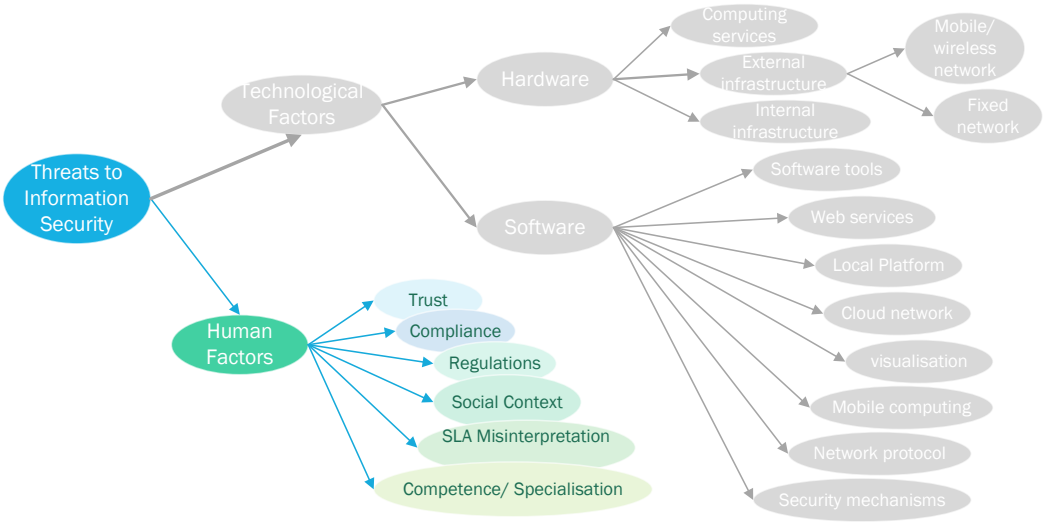

Figure 1.4: Taxonomy for identification of information security risks (Ahmed & Litchfield, 2016)

The unique cultural risk factors described in Chapter 4 violate trust, compliance, and regulations. The social context, Service Level Agreement (SLA) misinterpretations, lack of confidence and specialisation are shown in Figure 1.4. The interpretive research design approach, which is discussed in the following section, proposes a means to addressing the research question.

1.6 Research Approach and Findings

This section discusses the selection of the research method used in this study to answer the research question. The section also outlines the reasons why an interpretive research design is suitable for this study and its objectives.

Interpretive research design is centred on extracting empirical information and data for the purpose of analysis and evaluation. This method is appropriate given the sensitivity of the research question. The method determines the process of information gathering during this research and how it is presented in this report. Collected data comes from a variety of sources, including other research, articles, journals, video footage and primary sources, including personal experiences and in-depth knowledge of people who live in Tonga and are immersed in the culture.

In order to address the research topic, the research method provides two key tasks. The first task is to identify socio-political and cultural risk factors as security concerns to Tonga's hospital preparedness against cyberattacks. The second task is to evaluate and critically analyse how hospital information

security and the HIS are jeopardised by these cultural risk factors. These tasks offer the opportunity to make recommendations on the roll out of the digital HIS.

1.7 Thesis Structure

This section provides an overview of the thesis structure and how the study is conducted. This chapter provides background information about Tonga's hospital setting and explains the issues being addressed. This chapter also describes the research motivations and the importance of the findings to CS, Tonga's hospitals, and its citizens.

Chapter 2 presents a review of prior literature that focusses on the significance of the healthcare sector and why it is a target for cyber attacks. The motives behind cyberattacks and the consequences of weak security in hospitals. The significance of cultural influences on CS and data security, and whether culture has a positive or negative impact. The critical analysis of literature reveals gaps in the body of knowledge that directly address human risk factors with cultural and socio-political components.

To address the knowledge gap noted above, Chapter 3 presents the primary research question for this study. The method chosen for the study is an interpretative research design that incorporates pertinent industrial approaches and related studies.

The results of the interpretive research method are presented in Chapter 4. The findings from observations and documentation are described, starting with assessments of material from media articles, video archives, and private conversations on the research matter relevant to the study. Additionally, the researcher's direct experience of Tonga's culture and tradition are taken into account in this study. Documentation selection is from a broad range of sources as well as peer-reviewed articles, media articles, Government reports, NGOs and MoH reports.

In Chapter 5, the research question is addressed by critically analysing the results in Chapter 4 and connecting each finding to the major concerns outlined in the literature review. The implications of the results are covered in this chapter, along with recommendations for the reduction of risk associated with enhanced security and privacy of patient data.

Chapter 6 provides with a summary of the results and an outline of potential future research directions that will contribute to the general advancement of knowledge regarding cultural risks, security, privacy implications, and awareness.

1.8 Conclusion

This chapter introduces the study, the research subject, and its setting, which is the security readiness of Tonga's network of hospitals, as well as what cultural risk factors exist. This chapter also provides a synopsis of the thesis structure, the methodology, and the research technique. In the next chapter, a review of literature pertaining to the study topic are covered.

Chapter 2

Literature Review

2.1 Introduction

The objective of this chapter is to provide evidence from prior studies in CS culture, focusing on the identification of risk factors. The literature review demonstrates that there exists a research gap in CS culture in healthcare. The study focuses on the investigation of social culture in Tonga and how that is expressed as a range of cultural risk factors likely to lead to security threats to information security and the new digital HIS in hospitals.

This chapter demonstrates the importance of digital solutions for the healthcare sector, and how that elevates service and delivery to new levels of effectiveness (Lee, McCullough & Town, 2012). Studies identify new security threats that come with these high digital tech solutions (Wasserman & Wasserman, 2022) and in order to identify potential risks to CS, the chapter reviews the literature and studies in the fields of organisational culture and CS. Selected literature addresses research question in Section 1.5. The search selection and processing of literature are conducted through numerous online databases such as IEEE, Scopus, Google Scholar and AUT library databases to collect peer-reviewed materials. Literature selections are between 1993 to 2024.

The chapter is organised as follows, Section 2.2 defines, compares and contrasts CS and information security. Section 2.3 draws attention to the significance of the healthcare industry and hospitals as critical infrastructure and why strong security is necessary. Section 2.3.1 reveals the motives for why hospital ICT is an attractive target for threat actors, where top motives are financial gain, political motivation, the disrupted services. Section 2.3.2 emphasises the consequences of successful cyberattacks due to weak CS, that include financial loss, data loss, compromised reputation and trust, physical harm, and

significant impact on hospitals and patients.

Section 2.4 investigates CS culture in organisations, focusing on the importance of building the right CS culture. Section 2.5 presents an overview of common cultural factors of CS in organisations, and the dangers and cultural dimensions of CS.

2.2 Understanding Cybersecurity and Information Security

This section presents the definitions of, and contrasts between CS and information security. These two concepts are clarified so that the study is able to present the findings cogently.

While the terms information security and CS are used interchangeably, they are not the same. CS is defined by von Solms and Von niekerk (2013) as the effort to preserve an additional set of resources, primarily human and organisational, that are regarded to be more significant. Ioannou, Stavrou and Bada (2019); Da Veiga (2016) adds that it may be understood as accounting for shared ideals, convictions, and customary conduct concerning the defence of this wide range of elements. Astakhova (2014) state that information security culture is centred around preserving data and security where the two ideas are distinct components of a larger whole but are interwoven.

Over the past ten years, two early definitions influence the meaning of a culture of information security. Dhillon (1997) demonstrate that information security culture is influenced by human factors that contribute to the protection of information in an organisation and include behaviours, attitudes, and beliefs. Emphasising the role of employee behaviour in data protection, A. Martin and Eloff (2002) state that there is an assumption that employees are expected to incorporate information security characteristics.

While definitions of CS culture often focus less on information protection and more on general issues. For instance, in stating that the culture of CS promotes or inhibits safety, security, privacy, civil liberties of individuals, private and public organisations, Da Veiga (2016) include all aspects of security with people and organisations. More specifically, Ioannou et al. (2019) define CS culture as a set of directives for workers in a company for all circumstances that may affect the integrity of information. Information security culture, according to Nasir, Arshah and Hamid (2019), is centred on the improvement of employee information security behaviour while emphasising the protection of data assets. Both authors advocate for the encouragement of improved security practice by employees, particularly in relation to data and information. Similarly, Alshaikh (2020) describe CS culture as the protection of information processed by the organisation through compliance with information security policy. The definition also takes into account the need to understand how to implement requirements cautiously and attentively

requires regular communication, awareness, training and education initiatives. This is a view backed up by Mokwetli and Zuva (2018) who state that the idea concerns corporate policies and processes.

Focussing on a security culture or as an organisational subculture (Huang & Pearlson, 2019), a set of socio-cultural practices in which employee everyday activities naturally incorporate information security becomes apparent. Security awareness is viewed as a component of a security culture (Da Veiga, Astakhova, Botha & Herselman, 2020). Organisations that uphold and comprehend the security objectives have security awareness (Siponen, 2020).

Additional factors in a security culture include the engagement of employees and stakeholders which are expressed through their attitudes, assumptions, beliefs, values, knowledge and how those are used when they interact with organisational systems and procedures (Da Veiga & Eloff, 2010). The behaviours expressed through these factors are evident in the organisation's data protection policies and resources which evolves over time.

National Institute of Standards and Technology (NIST) NIST (2019), state that "information security protects data and systems from unauthorised use, modification, access, disruption, destruction, disclosure or ensuring availability, confidentiality and integrity." CS places high value on policy compliance while also encouraging individual involvement in organisational cyber protection. In this study, organisational CS culture refers to the attitudes, values, and beliefs that motivate employees to safeguard and defend the company from cyberattacks.

2.3 Cybersecurity in hospitals

This section examines hospital settings and reasons why the global health sector emerges as one of the most appealing targets for threat actors. Understanding the consequences of a successful cyberattack and the rationale for strict data and CS in the modern healthcare sector are crucial. The dramatic consequences successful cyberattacks on hospitals serve as a useful guide for understanding why healthcare security has to be at least equal to security in the financial sector.

The healthcare industry is essential because it is vitally important to society and the information it holds is not easily replaceable. Hospitals store some of the most sensitive information about patients, from patient care, diagnoses, sensitive information, personal identification data, payment details, and medications. In addition, the hospital provides data on births and deaths. When data are stolen, they are sold to create fake identity documents so criminals can perform illegal activities.

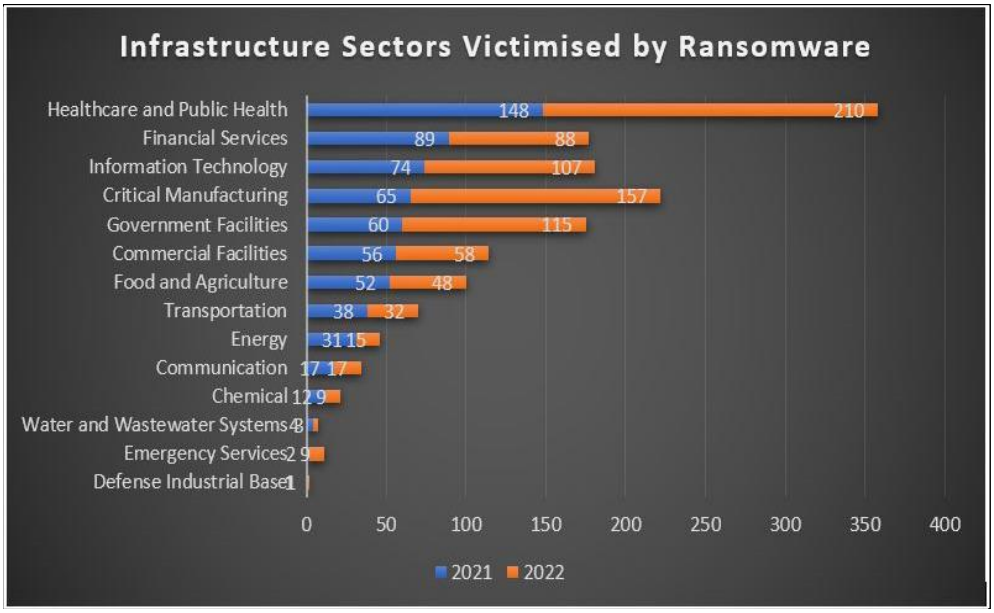

Figure 2.1: Sectors and Infrastructures affected by Ransomware Attacks. (Federal Bureau of Investigation, 2022)

2.3.1 Hospital becomes a targets of cyberattacks

The growth of the Internet and digital technology significantly increases connectivity at all levels and increases the attack surface of all organisations. Federal Bureau of Investigation (2022) reports that ransomware attacks are increasing, and Healthcare and Public Health reached the highest figure of attacks in 2022 by 210, an increase from the leading figure of 148 in 2021 (Figure 2.1).

Threat actors such as criminals, hackers, spies, hacktivists and ethical hackers take advantage of hospital vulnerabilities. Their motives vary by objective, level of qualification, and legality. If the motives of threat actors are known, then Hospitals must prepare to tackle the problem but that is not the case (Bhuyan et al., 2020).

Financial Motive

Financial gain is the most common motive for criminal attackers (Coventry & Branley, 2018; Luna, Rhine, Myhra, Sullivan & Kruse, 2016), where 91% of successful attacks account for information breaches (Bassett, Hylender, Langlois, Pinto & Widup, 2021) with data stolen from hospitals sold in the black market (Table 2.1). On the darknet, patient data records can be sold at around $50 each (G. Martin, Martin, Hankin, Darzi & Kinross, 2017) whereas the value of a complete medical set may be sold at a much higher price of $1000 Stack (2017); R. Smith (2023); Hernandez (2024). Ransom data, however, is

far more valuable (Healthcare Information and Management Systems Society, 2022) because these data can be resold to extort the same hospital.

Items Stolen	Number of Items	Price
Social security number	1	$1
Driver License	1	$20
Credit or Debit card	1	$5-$110
Online Payment Login	1	$20-$200
Diplomas	1	$100-$400
Medical	1	$1-$1000
Passport (US)	1	$1000 -$2000

Table 2.1: Stolen Medical Data and their monetary values on the black market

Stolen data may be used to solicit loans and other financial products that require identification documents (Coventry & Branley, 2018). Luna et al. (2016) adds that patient IDs are utilised to facilitate the application for cost-free medical insurance coverage such as Medicare. Healthcare Information and Management Systems Society (2022) reports that obtaining medical provider credentials significantly enhances the chances of breaking through hospital security networks or to facilitate unauthorised generation of medication orders and to profit from the sale of drugs (2018). It is evident that while professional certification holds nominal value, medical credentials demonstrate significantly greater worth.

Hacking is transforming into a full-fledged enterprise with ransomware being a prominent player (Kelpsas & Nelson, 2016). Cybercriminals adopt the role of entrepreneurs, selling data or hacking tools. The business is developing to the point where criminals present market data resembling legitimate businesses, such as rates of attacks, customer satisfaction feedback and success rates, and standard ransom prices.

Political Motives

Cybercriminals may be motivated by political objectives (Coventry & Branley, 2018). In times of international conflict, an aggressor nation may seek to hinder the target nation's provision of healthcare services to its people, sabotage medical devices utilised by its citizenry, or exploit confidential information for use against the targeting state. Bassett et al. (2021) demonstrate the incidence of espionage-related attacks accounts for 4% of all attacks. Examples include the launch of strikes to promote propaganda such as when the extremist group ISIS infiltrated the UK National Health Service (NHS) website in 2017 in which scenes from the Syrian Civil War were displayed (Sengupta, 2017).

G. Martin et al. (2017) point out that cyberattacks perpetrated by state actors and cross-border

cyberattacks represent some of the most formidable threats and identifying and deterring them is difficult. Domestic political motives may address local concerns such as Boston Children's Hospital attack in 2014 by actors communicating discontent about the management of a child custody case (Grimes & Wirth, 2017) and a ransomware attack against a Romanian hospital during the COVID-19 pandemic to protest the implementation of quarantine measures (He, Aliyu, Evans & Luo, 2021).

Disruption of Services

Cybercriminals may act to disrupt healthcare services (Giansanti & Monoscalco, 2021). Bergal (2022) emphasise that the healthcare industry is particularly susceptible to the detrimental effects of cyberattacks compared to other sectors, mainly because such attacks have the potential to not only compromise data security but also disrupt operational functionality (Cybersecurity and Infrastructure Security Agency, 2021) and even put hospital patients' lives in danger (S. J. Choi & Johnson, 2019).

The means of undertaking successful attacks include Denial of Service (DoS) attack (Cybersecurity and Infrastructure Security Agency, 2021), deploying ransomware, and compromising medical devices. A rationale for such attacks is personal satisfaction, which accounts for 5% of incident reports while a small proportion, 1%, is prompted by a perception of offence or grievance directed towards the medical institution or its practitioners (Bassett et al., 2021). However, Luna et al. (2016) argues that the incidence of cyberattacks perpetrated by vengeful employees has recently declined.

2.3.2 Consequences of weak security for hospitals

The following section discusses the significant consequences of a successful cyber attack in hospitals, highlighting why CS is critical in healthcare. Regardless of the motive or means of attacks, whether malware, ransomware, DoS Attacks, phishing, spoofing or an insider attack, the consequences would be substantial in cost, damage and scale. It is a fact that cyber attacks would affect not only hospitals' ICT and data security but critical services and patients' lives at risk (Bergal, 2022; Cybersecurity and Infrastructure Security Agency, 2021; S. J. Choi & Johnson, 2019).

Healthcare	Other Sector	Data Breach
231 days	204 days	before detection.
92 days	73 days	To contain the damage.
19 days	-	Fix and restore service
291 days	-	Data restore in multi-location

Table 2.2: Data breach and recovery timeline in the healthcare sector. (IBM Security, 2023)

The significance of prioritising IT security in hospitals and the health sector is highlighted as the highest number of attacks when compared to other industries. Healthcare data breaches commonly remain in the system for 231 days before detection compared to 204 in other sectors (IBM Security, 2023). It takes 92 days for cyberattacks to be contained in healthcare compared to 73 days in other industries and 19 more days of chaos to fix the problem and resume service to normality. It would take a more extended period of 291 days if hospital data is stored in multiple environments (Table 2.2). Healthcare experiences more prolonged periods of contamination and suffers more than any other industry in terms of cost, delay of service, loss of data security and privacy, and the direct risk to lives.

The areas most affected by security breaches and cyberattacks are financial costs, loss of data, ruins of reputations and trust, physical harm, and further impacts such as the pricing of products and services due to cyberattacks (Wasserman & Wasserman, 2022).

Financial Costs The strongest draw of cyberattacks targeting hospitals is money (Coventry & Branley, 2018; Williams, Chaturvedi & Chakravarthy, 2020). Healthcare Information and Management Systems Society (2022) indicate that financial harm is experienced in 20% of attacks. Furthermore, the healthcare sector stands as the leading industry in terms of financial investment directed towards addressing data breaches, amounting to an average of $7.13 million globally. In contrast, the average cost of security breaches across a range of industries in 2020 is USD3.86 million, increasing to USD4.45 million (IBM Security, 2023).

Over the past decade, the highest-ranking position within the United States has remained consistent, with a notable upward cost trend. The costs are experiencing a significant increase of 10.5% within just two years in the IBM Security (2020) report, and the number is going up again to a 15% increase over three years in the IBM Security (2023) report.

Financial burdens arise as a consequence of cyberattacks (Peterson, Adams, Sanders & Sanford, 2018), encompassing the need for emergency protocols like shifting from electronic to paper-based systems for recording patient data, payment of ransom fees, expenses associated with repairing or restoring affected systems, public relations efforts, legal expenses, communication costs, financial security losses, rebooking costs, staffing levels for breach response, costs associated with changing or replacing the CS system, training costs for CS (Pullin, 2018), and fines by security oversight agencies as punitive measures. Furthermore, IBM Security (2023) demonstrate the importance of acknowledging that every instance of a data breach can potentially disrupt and erode customer trust significantly, resulting in a costly recovery process for the healthcare sector.

Data Loss G. Martin et al. (2017) indicates that financial information and medical records exhibit a distinctive characteristic, that they cannot be easily restored to their original state if stolen or damaged. Hospitals may be willing to pay a ransom for data breaches, but hackers might continue to withhold information until money is received. Alternatively, criminals may opt to sell the data to other hackers who would carry out subsequent ransoms or offer it to darknet customers interested in acquiring sensitive information.

Furthermore, C. Smith (2018) adds that attackers may choose to return a portion of the compromised data or provide a modified version that deviates from the original dataset. According to US privacy regulations, hospital data subject to ransom or other attacks is deemed unreliable or, at the very least, permanently compromised (Dullea, Budke & Enko, 2020).

Reputation and Trust While the most widely discussed repercussion of cyberattacks on hospitals is financial loss (Wasserman & Wasserman, 2022), an equally significant and far-reaching consequence is the impact on the hospital's reputation (Williams et al., 2020). The occurrence of a data breach in healthcare settings can generate a profound distrust between patients and healthcare providers (Giansanti & Monoscalco, 2021). The decline in patient trust reduces the inclination for patients to offer personal information to healthcare providers, including potentially vital clinically relevant information (G. Martin et al., 2017; Coventry & Branley, 2018). The absence of established protocols in approximately 67% of hospitals to support patients whose confidential information is compromised, Ponemon (2016) indicate that it is likely to exacerbate the erosion of trust in the aftermath of a cyberattack.

Physical Harm The prospect of inflicting physical harm on patients (Coventry & Branley, 2018; Williams et al., 2020; Giansanti & Monoscalco, 2021) is a potential consequence of an attack. Healthcare Information and Management Systems Society (2022) support this view, stating that 55% of recent attacks target hospital networks and services, whereas 18% of these attacks directly target or cause damage to essential systems involved in providing medical care. Healthcare Information and Management Systems Society (2022) state that the occurrence of certain events results in severe harm to patients (Bergal, 2022). Healthcare Information and Management Systems Society (2022) describe how digital hospital equipment at the ancillary level, such as computer-operated elevators used for patient or lab sample transport and HVAC systems responsible for maintaining sterility in operating rooms, have the potential to be shutdown or malfunction. Moreover, Tully, Selzer, Phillips, O'Connor and Dameff (2020) state that reallocation of resources

will be necessary to address an attack, resulting in diminished availability of resources for medical attention both during and after the incident. Coiera, Aarts and Kulikowski (2011) show that downtime in hospital systems can impact patient care.

The harmful effects of the WannaCry attack on the NHS in the United Kingdom (Grimes & Wirth, 2017) demonstrate the tangible effects on clinical care, with patients relocated to alternative facilities while redirecting ambulances to other hospitals. Bergal (2022) discusses how attacks have detrimental effects on patients in time-critical emergencies who are redirected to facilities located further away and those receiving medical procedures and surgery. Clarke and Youngstein (2017) report on refrigerators electronically locked with vital supplies being unobtainabale during the attack.

Tully et al. (2020) explains that in the ongoing struggle between security, availability, and usability, cyberattacks can have a major impact on hospitals' clinical results. In the United States, the average yearly decline in the 30 day mortality rates from Acute Myocardial Infarction (AMI) was 0.4% between 2011 and 2017. However, in hospitals that experience data breaches, the rate of deaths within 30 days after an AMI remains stable but shows an increase of 0.34 to 0.45% annually for a period of 2–3 years. S. J. Choi and Johnson (2019) theorise that differences in CS practices between hospitals may contribute to data breaches and prompt hospitals to implement new and unfamiliar CS protocols, leading to frustration and error. Regardless of the underlying reason for the statistics, Wasserman and Wasserman (2022) highlights the study's importance to patient safety.

Further Impact Cyberattacks targeting a single institution can have far-reaching consequences for other global entities. Wasserman and Wasserman (2022) highlight that an incident occurring in one hospital cyber domain may impact on the resources of other hospitals, their ability to function, and digital security.

Examples not necessarily related to healthcare but demonstrating downstream effects include The Saudi Aramco petroleum and gas corporation temporary shutdown due to a phishing email in 2012 (Pagliery, 2015). The company replaced 50,000 corrupt hard drives which resulted in a global price hike and global disruption of the drive supply chain for five months. IBM Security (2020) and IBM Security (2023) reports 60% and 57% of companies respectively have experienced price rises for product or services due to data breaches.

2.4 The importance of having the right culture for security

This section discusses cultural aspects of organisational management in healthcare. No case study can be found that address organisational cultural factors from an ethnic culture similar to Tonga, so selection of literature is based on common cultural factors in organisations. To isolate risk factors in hospitals, this section also discusses the right culture required to secure CS in organisations (Huang & Pearlson, 2019).

Healthcare facilities seek to protect resources from cyberattacks and hackers Huang, Siegel and Madnick (2018). The existing body of knowledge regarding CS culture primarily focuses on ways organisations can enhance CS culture (Reegard, Blackett & Katta, 2019; Cremer, 1993). Even the most sophisticated of technological protection cannot shield a company from a cyberattack if its employees do not exercise caution and self-preservation. Choudhry, Fang and Mohamed (2007) explains the meaning of culture as it relates to organisations and safety, particularly when it comes to developing safety. Features include a positive safety culture, safety culture models, levels of aggregation, and safety performance. A safety culture is generally believed to have an impact on worker attitudes and behaviours.

The most challenging security component is the insider threat resulting from human behaviour (Huang & Pearlson, 2019; Bassett et al., 2021; Samy, Ahmad & Ismail, 2010) and the primary agents of cyberattack in the healthcare industry are employees. All it takes for an attacker to gain access to a company's computer systems is for one employee to click on a phishing email. Once inside, an attacker can destroy vital infrastructure, as demonstrated by the WannaCry virus (Grimes & Wirth, 2017). The problems are due to employees failing to follow CS protocols (Swede, Scovetta & Eugene- Colin, 2019). Healthcare Information and Management Systems Society (2022) states the cyber events caused by employees accounts for 40% of attacks. IBM Security (2023) adds that approximately 27–35% of cyberattacks in 2020 are the result of human error. It is essential that healthcare is prioritised with a balance between patient safety and system protection.

Creating an organisational culture that values CS can help shape employee behaviour and boost cyber resilience (Choudhry et al., 2007). A culture of CS provides guidance on procedures, guidelines, and unwritten rules. In explaining why investment in CS is necessary, the Chief Information Security Officer (CISO) of Liberty Mutual says that companies run the risk of compromising their investment if hackers gain access to systems. Similarly, The first request for information from the global executive overseeing risk and security management at Johnson and Johnson was to ask what people and culture strategy the company follows (Huang & Pearlson, 2019). However, CS culture can be challenging to define, cultivate, and measure (Leidner & Kayworth, 2006; Da Veiga, 2016). A foundation for a CS culture model includes

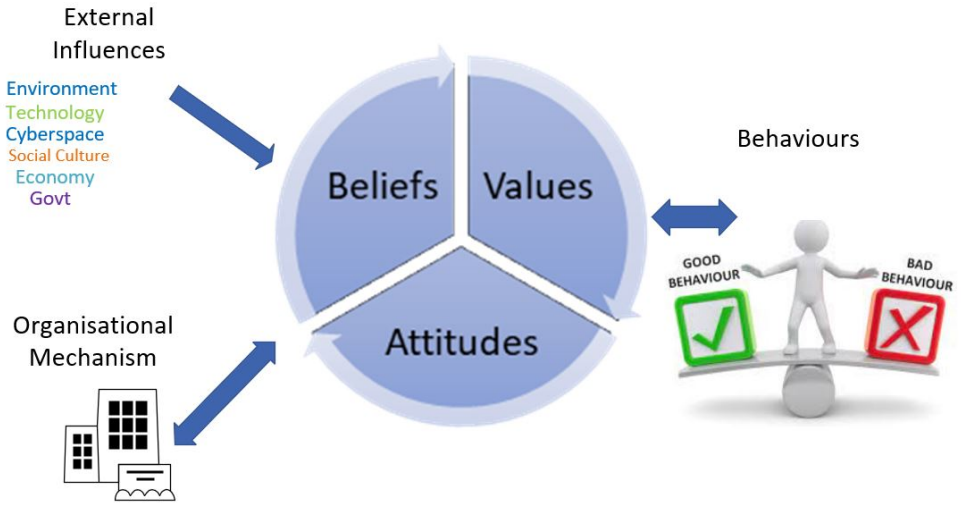

Figure 2.2: The conceptual framework of a cybersecurity culture (Huang & Pearlson, 2019)

the analysis of organisational cultures by type, for example, those that establish strong safety cultures (Carrillo, 2010) in which employees know how to be safe and reduce the risk of accident.

2.5 Common Cultural Factors in CS

This section presents the common cultural factors in CS from an organisational context. These factors reveal the significance of CS culture in the health and operation of organisations, including hospitals. Common factors include: external influences; CS as a central part and force in the organisation; leadership's ability to foster a CS culture; CS enabling business and staff contribution to CS.

A cultural framework is one that establishes a connection between employee conduct and culture while also considering the impact of managers and external influences on CS culture (Huang & Pearlson, 2019; Cremer, 1993) (Figure 2.2). Culture and management have a reciprocal influence on each other such that management drives CS behaviour. Similarly, there is a two-way relationship between employee behaviour and culture. However, culture is greatly influenced by external factors that are outside the direct control of the organisation, such as regulatory compliance, national or local customs, and the activities of other organisations.

2.5.1 Cybersecurity Culture Is Central

CS culture is a central component to the model in Figure 2.2. While most are aware of unwritten rules, few can express values, attitudes, and beliefs. Nonetheless, these are discernible through the behaviours of

individuals, groups, and leaders. Marotta and Pearlson (2019) states that culture plays a fundamental role in every aspect of an organisation, even in situations where the significance of cultural values might appear to be overlooked. An organisation's culture refers to the implicit guidelines that influence the actions and conduct of every team member. An organisation's culture is created by sharing values, attitudes, and beliefs, influencing the thinking, emotions, evaluations, and actions of executives and employees within different departments (Huang & Pearlson, 2019). Evaluating a company's culture involves examining its hierarchy, managerial decisions, long-term objectives, and the conduct or behaviour of its employees.

Alshaikh (2020) recommend establishing a CS champion network or hub to assist with spreading CS awareness among employees and be the point of contact between ICT and the rest of the employees. A CS champion network is necessary in large organisations like hospitals. This team is on the front line in spreading CS awareness, they are the go-to person providing feedback to ICT. This team must have the initiative and the ability to get the attention of executives and win support and obtain necessary resources (Schein, 1996; M. Choi, 2016). The team receives training from ICT in CS policy. CS updates are maintained through regular meetings with ICT.

2.5.2 Culture is Created by Leaders

Culture is frequently established and controlled by an organisation's leaders, where they exist as a point of interconection to reach agreement Marotta and Pearlson (2019); Huang and Pearlson (2019); Schein (1996); M. Choi (2016); Cremer (1993). Schein (1996) suggests that the primary role of a leader is to establish the organisational culture and Marotta and Pearlson (2019) point out that possessing the skill to effectively handle and oversee the culture is a crucial capability of a leader.

Leaders that positively influence the growth of a shared understanding within the organisation typically align those goals strategically with the business (Huang & Pearlson, 2019; Cremer, 1993). It is more common for leaders to initiate actions that boost CS and share information with others within the organisation when these leaders know about keeping the organisation cyber secure. The expectations of management and leadership are critical to ensuring that a security culture is a high priority in the organisation and its culture. Management support may be divided into two categories: A dedication to CS, and an emphasis on the significance of information security and the need for full executive support and involvement (Masrek, Harun & Zaini, 2017).

However for staff, competition for time exists and Uchendu, Nurse, Bada and Furnell (2021) state that employees do not view CS initiatives as important if management support is not provided. For example, resources ought to be available and allocated as required and management needs to ensure that resources

are appropriately managed in addition to directing employee attention toward CS culture initiatives.

Campos and Reich (2019) identify factors that influence the politics of policy implementation in the health sector in developing countries. These factors are leadership, budget, beneficiary, bureaucracy, interest groups and external actors. These factors exist at the top and middle classes of society in general, where manpower and resources are required to enable the implementation of policies. CS policies and procedures need to be comprehensible enough for employees to implement (Uchendu et al., 2021), otherwise employees will not access them and risk breaching policy (Greig, Renaud & Flowerday, 2015). Olivos (2012) notes that security policies failing to distribute among staff are scattered across multiple files and documents. According to the studies, these issues indicate serious problems regarding the current state of security culture. Management and IT departments guarantee that workers are exposed to the most recent and appropriate security policies required for the company domain and possess the requisite policy knowledge.

2.5.3 Cybersecurity Enable Business

Organisations face difficulties when obtaining senior support for security because security is frequently perceived as a barrier rather than an enabler of business. This demonstrates the need for an industry-wide shift in perspective regarding CS. Legislation that applies heavy fines on businesses found to have inadequate security, such as the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR) is driving this change (Sirur, Nurse & Webb, 2018; Forbes, 2020), in addition to the growth of cyber insurance, which serves as a financial safety net during a cyberattack or crisis (Nurse et al., 2020). These two ideas have pushed CS up to the boardroom table, affecting an organisation's longevity.

A critical factor for CS is integration with business requirements, customer service, and recognition that this develops over time. One illustration of this, according to Marotta and Pearlson (2019), is how the responsibilities of CISO change, moving beyond overseeing CS projects to taking on new responsibilities such as strategy management, policy, governance, and engaging with external regulators. Such change effectively communicates that CS is not contradictory to business goals but rather supports and should be seen as a crucial aspect of business responsibilities. Key to success is for senior managers to prioritise CS when management sees the values of this field in the company (Huang & Pearlson, 2019). Leaders' decisions regarding resource allocation and strategic discussions reflect this shift. Executives' participation describes the direct involvement of top management in CS-related endeavours. Communication of CS policies, attitudes and specific organisational security measures, such as participation in training, game

activities, financing and other CS activities, are ways to participate and experience. To increase security consciousness and influence conduct amongst staff, it is important that internal and external efforts to raise awareness are conducted (Alshaikh, 2020). A CS campaign can include meetings, work promotions, and training inductions to increase awareness of the value of adhering to security policy of organisation's and to provide informative and entertaining ways to keep the organisation informed.

2.5.4 Employee Contributions to Cybersecurity

Marotta and Pearlson (2019) demonstrate that organisations must ensure that staff are actively contributing to its customer service defences and that executives prioritise the creation of a CS culture. To instil the significance of security as a fundamental aspect of working for the company, the approach needs to be the company's main strategy. The strategy ought to emphasise values, attitudes, and beliefs.

It needs to be understood that CS addresses more than technical problems (Huang & Pearlson, 2019). Businesses ought to be able to rely on employee behaviour to defend against threats or to stop active cyberattacks. Employee behaviour determines how vulnerable a company is to successful cyberattacks where staff may demonstrate "in-role" and "extra-role" behaviours. An employee's performance in action and activities is referred to as in-role CS behaviours and include reduction of computer abuse, adhering to formal organisational security policies, and preventing policy violations (Bhuyan et al., 2020). Extra-role CS behaviours are actions and pursuits that a worker engages in outside the scope of the employment contract. Examples of extra-role behaviours may include voicing, which is starting a conversation to share knowledge and insights to advance CS, and helping, which is opting to work cooperatively to support others who might have CS-related enquiries. Extra-role CS practices benefit because the internet is a complex environment with threats at all organisational levels. Security leaders appreciate fresh perspectives and information on newly discovered vulnerabilities and strategies for consistently enhancing organisational CS.

To build and maintain a strong CS culture, rewards and sanctions in CS awareness programmes are tools that may be applied (Blythe, Gray & Collins, 2020). It can be challenging to determine the appropriate level of punishment for employees who disobey and breach security protocols, as well as to address the needs required when a high-performing employee struggles to integrate into the organisation's security culture. Alshaikh (2020) suggest establishing a network of champions to promote security awareness and policy implementation within an organisation. Champions play a crucial role in spreading security messages and supporting employees with security protocols.

2.5.5 External Influences

External factors influence individual or organisational attitudes, beliefs, and values regarding CS. For instance, people become more aware of the risks associated with CS the more the public press covers cyber breaches. Additionally, in certain sectors of the economy, organisations are required by governmental and regulatory bodies to prepare for cyberattacks. For instance, businesses that follow the GDPR are given preference over those that do not. This regulatory framework requires organisations to designate a data protection officer.

Societal CS culture encompasses the values and customs in the society that an organisation functions. Huang and Pearlson (2019) argues that variations between nations and societies influence how individuals perceive online threats, for instance, whether countries prioritise data protection as a crucial societal value and how they are reflected in organisational beliefs in nations that align with this cultural perspective. Whereas organisations in countries that adopt a more relaxed approach reflect a similarly relaxed attitude towards CS.

Furthermore, national culture as a factor suggests that CS culture at a national level is instrumental in developing a corporate CS culture (Alhogail & Abdulrahman, 2014; Ruhwanya & Ophoff, 2019; Da Veiga & Martins, 2017; Da Veiga et al., 2020). To express this, Gcaza, Van Vuuren and Von Solms (2015) propose an ontology of national CS culture, including SMMEs and staff training. To demonstrate the effectiveness of this approach, Bada, Von Solms and Agrafiotis (2019) discusses the state of national CS literacy across African nations, urging participation from stakeholders in various sectors, including SME staff and executive board members. There exists a cascade effect from this strategy where national CS efforts contribute to organisational CS culture. However, creating a national custom is far more complex than creating an organisational culture.

2.6 Conclusion

The literature review presents an overview of the research on CS in healthcare and culture in organisation that is applicable in healthcare. While a growing body of research touch different areas of CS, this study finds that there is a lack of non-technical research and literature in CS. The research also finds a lack of interpretive methods in the area of CS.

The literature review discovers that CS culture tends to be western oriented and is generally focused on the organisational setting and management. This research clarifies that while organisational culture influences on CS is well-studied, the specific impact of ethno-cultural factors is a newer area of research.

This review did not find any studies that address ethno-cultural, factors and this study is the first that addresses the unique case of Tonga. Additionally, the review discovers a gap in the understanding of CS culture and a lack of research on cultural risks in the context of national or ethnic cultural influence on CS in organisations. This research gap leads to this research question to address the issue.

Research Question

What are the cultural risk factors in the Tongan cultural context that identify as security threats to the CS readiness of digital HIS in Tonga?

This study researches Tonga's national culture with the purpose of uncovering the cultural risk factors identified as threats to CS readiness in hospitals in Tonga. There is currently no known study or literature on national and ethnic cultural factors to identify their influence and potential threats to CS and information security.

The next chapter presents the research method to investigate cultural risk factors in Tongan society that could pose a security threat to the CS readiness of hospitals. These cultural factors are national and ethnic cultural traditions unique only to Tonga. The cultural factors involved are either gender discrimination in nature or corruption in nature, similar to the universal concept of nepotism, favouritism and faction, which enables security breaches or cyber-attacks in hospitals or other organisations.

Chapter 3

Research Design and Methodology

3.1 Introduction

The previous chapter identified a gap in the body of knowledge about the influence of cultural factors on digital HIS, especially in the case of ethnic cultures from around the world. In this research it is in the context of Tonga. This chapter presents and discusses the methodology that addresses the research problem: interpretive research. The selection focuses on the research question that is restated from the previous chapter.

Research Question

What are the cultural risk factors in the Tongan cultural context that identify as security threats to the CS readiness of digital HIS in Tonga?

This chapter is structured as follows: Interpretive research as a method of selection is defined and described in Section 3.3. This method's suitability for this research is justified in the remaining sections by the principles it adheres to in Section 3.3.1 to ensure its trustworthiness and avoid bias. Research rigour is discussed in Section 3.3.5, addresses the dependability, credibility, confirmability, and transferability of the research findings are convincing. Data access and collection processes are presented in Section 3.3.3 with a section describing the use of anonymous sources in this research, and the reason for this decision is also explained.

3.2 Selection of methodology

Chapter 2 identifies a gap in research and literature available in the area of social and ethnic cultural factors and how they affect CS. The gap highlights the need for information to help secure CS in the new hospital digital system as part of the recent eGovernment rollout. Investigating Tonga's social culture and socio-political phenomena and how they affect CS would be the first of its kind. The research topic is sensitive because it involves investigating the vulnerability of Tongan culture and tradition that reveals cases of corruption in the public sector.

Finding a suitable methodology for this research is challenging because of the sensitive nature of the research topic also the difficulty of gathering data from research environment in Tonga. This chapter shows why the selected method is the right method to use which involves sourcing data from the literature on Tongan culture and Tonga's socio-political relationships regarding its influence on CS in Tonga.

Sourcing data and information through interviews and surveys from key people in Tonga is challenging as requests for comments are ignored or these people are unavailable. Civil servants, including healthcare employees, are aware of employment commitment and would avoid making comments in the media and academic research interviews for fear of violating employment policy or legal breaches. The selection is therefore to observe from a distance and conduct a qualitative analysis confirmed by Geertz (1985) who refers to the experience-distant concept, that a specialist might employ to forward scientific, philosophical, or practical aims.

However, some individuals with roles relevant to the research provide comments related to cultural risks in the workplace but ask to remain anonymous (discussed in Section 3.3.4). The selection of data sources, forms, and methods generate excellent outcomes that are not only logically connected to the research setting but also provide the information required to answer the research question.

3.3 Interpretive Research Design Structure

This section describes the selection of the research method and why it is the appropriate method for this research. Interpretive methodology is chosen with the description of principles in Section 3.3.1, and benefits and challenges in Section 3.3.2. Section 3.3.3 covers the access and data collection process, while the application of anonymising sources is discussed in Section 3.3.4.

Interpretive case research design facilitates an in-depth investigation into the socio-political and cultural aspects of Tonga, making it the appropriate method for this research. The primary objective of the study is to identify vulnerabilities and potential risks that may compromise the CS, data security, and

privacy of hospital systems in Tonga. This research study aims to discern specific details, contextualise inferences, and develop a comprehensive understanding of Tonga's social and political culture. Through this exploration, the research aims to identify vulnerabilities that may arise as potential risks to the CS of hospitals in Tonga, thereby enhancing the knowledge in this domain. In the field of social sciences, it is the expectation that a study assumes the role of direct observation in social settings and adheres to a stance of impartiality (Schwartz-Shea & Yanow, 2013). Similar to other interpretive methodologies, the ability to extract signifying constructs from case studies is heavily reliant on research acumen in observation and integration.

The term interpretive research is often used casually and interchangeably with qualitative research despite there being significant differences between these concepts. Kuhn and Musgrave (1970) describes interpretive research as an approach that focuses on the idea that social reality is not a single objective concept but is shaped by how people perceive and interact within its social surroundings. This viewpoint proposes that understanding social reality is best achieved by analysing it within its socio-historic context and considering the participants' perspectives.

Interpretive research perceives social reality as inherently embedded within and inseparable from its surrounding context (Kuhn & Musgrave, 1970). As a result, the research actively involves making sense of things rather than testing hypotheses as it strives to understand the world around it. This idea is distinct from the positivist or functionalist viewpoint which believes that reality is primarily unaffected by its surrounding environment. From this viewpoint, an examination should be carried out separately and strives to analyse the nature of reality by focusing on specific aspects and using objective techniques such as standardised measurements. The decision to pursue either interpretive or positivist research depends on the philosophical considerations about the nature of the phenomena and the field of study as the most effective approach for studying it.

Considering factors that determine the nature of this study, qualitative research methods are appropriate as the secondary approach for this research. Bhattacherjee (2012) demonstrate that qualitative research is appropriate for the empirical nature of data acquisition and analysis. Qualitative research relies on non-numeric data related to the study question, such as literature, data, and observations. Including quantitative data can enhance precision and facilitate a more lucid comprehension of the phenomena under investigation.

3.3.1 Principles of Interpretive Research Design

Engaging in Interpretive Research necessitates adherence to established principles, (Bhattacherjee, 2012). This section presents five principles relevant to this research:

1. The naturalistic inquiry in which social phenomena are locally situated. Interpretative inquiries assume that social phenomena are expressed by the social environment and therefore the historical context. Thus while looking for clarification about phenomena, relevant characteristics are examined but given the local context, conclusions may not be generalisable.

2. The person conducting the study is often immersed in the social setting of the investigation, and in this instance remotely, is recognised as an intrinsic part of the data gathering process. The method requires drawing on personal Tongan cultural knowledge and experience. Additionally, including anonymous sources and individuals' insights, knowledge, and experiences concerning the social context is essential in facilitating an accurate interpretation of the phenomenon under investigation. Simultaneously, participants must exhibit conscientious self-awareness regarding individual biases and preconceived notions, ensuring the absence of biases compromising the capacity to deliver an impartial and precise representation of the phenomenon.

3. Observations are subject to interpretation by the participant's immersion within the specific sociocultural milieu. The process of interpretation must be conducted at dual levels. The initial tier entails observing or encountering phenomena through the subjective viewpoints of participants.

4. To provide description or narrative account of the phenomenon of interest, this stage involves comprehending the significance of participant experiences and unpacking the rationale of participants behaviour. So that readers can understand and relate to the case, the researcher uses expressive language to report and investigate participant non-verbal and vocal communication styles and depict their thoughts and experiences. The use of images, representations, and other forms of speech is widespread in interpretive research.

5. Interpretive research focuses on comprehending and giving meaning to the ever-changing social processes rather than seeking definitive answers. Thus, to comprehensively observe and understand the complete development of phenomena under investigation, this study requires a complete immersion in the study location for a significant period.

3.3.2 Considerations of suitability

Interpretive research demonstrate is ideal for investigating underlying factors that contribute to complex and interconnected social processes, such as relationships between companies or office politics (Bhattacherjee, 2012). The methodology provides assistance in constructing theories in areas that lack prior theory or where existing theory is inadequate. Additionally, interpretive research is suitable for examining events or processes specific to a particular context and may be distinct or unusual. Interpretive research has the potential to identify captivating and pertinent inquiries and concerns, which can further contribute to future research endeavours.

However, interpretive research is not without its unique hurdles. When it comes to gathering data and analysis, interpretive research requires more time and resources compared to positivist research (Walsham, 2006). Insufficient data can produce inaccurate or premature conclusions while excess data can overwhelm the research and hinder effective processing.

Furthermore, interpretive research necessitates proficient research capability to perceive and comprehend intricate social occurrences from the viewpoints of those involved while also harmonising these individuals' various perspectives. The research must refrain from injecting bias or preconceived notions into the research interpretations. But not all participants or sources of information are equally reliable, impartial, or well-informed. Some may have undisclosed political motives, resulting in distorted or erroneous perceptions. The role of interpretive research is to skilfully perceive and comprehend the genuine essence of an issue, even when it is concealed or influenced by personal biases or hidden agendas.

Therefore, due to the highly dependent nature of conclusions derived from interpretive investigations, replicating or generalising findings poses a significant challenge. In some instances, interpretive research might not respond satisfactorily to the research inquiries or accurately anticipate future behaviours (Bhattacherjee, 2012).

3.3.3 Access and Data Collection Process

This section presents the access and data collection process used in the interpretive research method. Observation and documentation are described, while the decision to include anonymous sources is explained in Section 3.3.4 as opposed to conducting interviews.

Unbiased external observation employs direct observation to collect data. The researcher refrains from becoming directly involved in or participating in politics and cultural bias (Schwartz-Shea & Yanow, 2013). In this study, observations of Tongan culture seek to identify risk factors considered a security

threat to the new digital HIS or ICT in Tonga's hospitals. Drawing on extensive first-hand observations and holding a priori deep understanding of Tonga's social structures and culture greatly benefit the study.

Additional sources include documentation that provides essential social, cultural, and political events, including corruption charges in Tonga. This documentation comprises journals, articles, and online video footage from various local and international sources, including Matangi Tonga, Tonga Times, Kele'a, and New Zealand media. Additionally, documentary sources include Government reports and presentations on e-government initiatives, media and video footage (YouTube) that provide information on Tonga's social and cultural issues, as well as local and international news concerning the research topic. Research data provide a deeper understanding of Tonga's social and cultural environment and its threats towards information security and the ICT or HIS in Tongan hospitals (C. Smith, 2018).

An interpretive view of data collection is described as produced data that results from other people's work (Geertz, 1985). Data collection is based on a descriptive examination of Tongan culture, dangers and supports are identified using information presented in the next section.

3.3.4 Anonymous Sources

The decision to abstain from conducting interviews is established in advance. While the need for AUTEC approval is no longer a requirement, participants that have knowledge of the research volunteer information on the condition of anonymity. These individuals cover a range of qualified IT employees with excellent knowledge of the Tongan culture and connections to Government ministries and the hospital network.

The reasons for abandoning interviews and surveys are motivated by a multitude of factors. The primary determinant lies in the level of sensitivity to the subject matter under investigation. The exploration and unveiling of vulnerabilities pertaining to social, political, and cultural aspects of Tonga's society is a subject that necessitates utmost caution and sensitivity. In scrutinising the socio-political and cultural aspects of an institution and civilisation with an extensive history spanning thousands of years, it becomes pertinent to contemplate the qualifications and suitability of the person behind the research for engaging in such a public discourse.

Tonga's socio-political and cultural issues are delicate, hence most issues are avoided even when inquired about. This affects the general population and civil servants, who face potential repercussions, risking job security or reprimands, for broaching these topics. This is the reason why none of the correspondence to key people in Tonga were replied to and requests for information that would assist in this research were declined. Participation or abstention from responding to queries are due to concerns

about potential risks of legal and contractual breaches or consequences of being subject to ridicule or being ostracised. Free and open discussion of Tonga's social culture and its susceptibility is widely regarded as disrespectful, especially in the public domain.

Additionally, any criticism of Tongan culture is met with substantial challenges, potentially impeding the ability to gather pertinent information from governmental and non-governmental sources. Individuals possess an awareness of the potential consequences associated with this trajectory, namely the emergence of corruption and cultural problems within the government and its respective entities, particularly the MOH, in the context of this study. Tonga's socio-political and cultural aspects have long been subject to scrutiny from the pro-democracy movement. Therefore a neutral standpoint must be maintained and refrain from including bias, while presenting the veracity of findings in Chapter 4 and engaging in discussions in Chapter 5.

Sources involved in this study are anonymised by utilising of methods commonly used in the healthcare industry. This is the removal of all information or metadata that could be used to identify a person, making these sources untraceable. The metadata include names, age, gender, workplace and location (ENLITIC, 2023; Garfinkel, 2015).

Anonymous sources are described in Section 4.2 and individuals are titled AS1, AS2, AS3 and so forth, with positions relating to ICT, Government ministries, connection to aristocracy, and level of expert knowledge of the Tongan culture and current events in Tonga.

3.3.5 Rigour in Interpretive Research

This research exploits a wide selection of real-life examples and evidence, regulations, laws and international standards in CS such as ISACA (ISO, 2013a), ISO IEC 27001 and ISO 27002 (ISO, 2013b). These standards frameworks are used as a compass and provide guidance on identifying cultural risk factors in both the social and socio-political arena.

In legal standards, a selection of examples from other countries are used to support this research. For example, HIPAA, a powerful CS legislation in the United States, safeguards the integrity and security of patient information from unauthorised access and illegal dissemination without the patient's consent (US Department of Health and Human Services, 1996). The HIPAA is a federal law effective across the United States that bans and makes it illegal for health employees to access and disclose patient information without consent. The consequences are internal disciplinary, loss of a job or legal action.

The New Zealand Privacy Act of 2020 (Justice, 2020) protects individual rights to privacy, and New Zealand's Crimes Amendment Act of 2003 (Justice, 2003) is designed specifically for crimes involving

computers. New Zealand Cyber Security Strategy 2019 (Department of the Prime Minister and Cabinet, 2019) is evidence of the Government's commitment to CS worldwide. Tonga does have legislation that covers computer and digital crimes, such as the Computer Crimes Bill 2019 (Government of Tonga, 2019), but it does not cover patient data privacy and confidentiality. The cultural risk factors discovered in this research either contribute to cyber threats that are liable under the law or are ethically unjust according to the Codes of Ethics and Conduct in Healthcare Ethical Standards worldwide. Regulations and the law in different jurisdictions guide this research method in approaching the research question. Relevant legislation, international standards in CS, and Codes of Ethics in this section help shape discussions over the research findings.

Previous research on similar topics is reviewed to ensure method validity (Chapter 2) and presents existing issues in general cultural and socio-political risks in CS. However, the case of Tonga is unique wherein socio-political and cultural factors in the Tongan context and the link to CS have never been examined previously. The purpose of this study is to help Tonga close the gaps in detecting and managing cultural and socio-political risks in CS.

This research design utilises a set of risk criteria adopted from (Ahmed & Litchfield, 2016). The taxonomy (Figure 1.4) categorises risk factors for Cloud Technology into classes based on human and technological factors. The taxonomy refers to human risk factors and assists in identifying cultural and socio-political risks and how to classify them (Chapter 5). Cultural risks come under human factors that include trust, compliance, regulations, competence and specialisation, SLA misinterpretation and the social context. The risks discovered in the study match the human factor categories in the taxonomy. Each cultural and socio-political vulnerability discovered can be linked to security and privacy breaches of HIS systems and data information. For example, social privilege in Section 5.2.1 is linked to data leaks, breaching hospital work policy and regulations, breaking the law on CS and data privacy, breaching trust among hospital employees and patients as well. Social privilege also reflects the weak links and vulnerabilities in hospital management and what needs to be done to mitigate the problem.

The cases of vulnerabilities are extracted from Tonga's socio-political and cultural context and are directly applied to the taxonomy to identify the risk type each belongs to. The discussion of each vulnerability and the associated risk type each is linked to are covered in Chapter 5.

3.4 Conclusion

This chapter presents the rationale for the selection of interpretive research as the chosen methodology of this study. The rigorous application of this method and its trustworthiness are reinforced through dependability, credibility, confirmability and transferability. This study requires a thorough interpretation analysis through qualitative methods of cultural and socio-political risk factors in Tongan society that identify as a threat to CS in order to answer the research question. The access and data collection process is carried out through observation and documentation, video footage, articles and anonymous sources. The next chapter presents the findings from the data collection processes and offers an analysis of data.

Chapter 4

Analysis of Qualitative Data

4.1 Introduction

Chapter 3 establishes the research methodology that guides this research into achieving the findings in this chapter. The findings obtained from the investigations are cultural risks unique only to Tonga and socio-political risk factors that this study identifies as threats to CS readiness of the digital HIS in Tonga's hospitals.

This chapter analyses five cultural risks and two socio-political factors. Section 4.4.1 identifies Tonga's cultural stratification as a risk factor and a threat to CS. Section 4.4.2 uncovers centralisation leadership and networks in the new e-Government as a security risk factor. Section 4.4.3 presents the analysis of the Tufakanga– a cultural division of labour as a security threat. The cultural concepts of kinship, kainga and fahu privilege as a security risk are present in Section 4.4.4. The analysis of gender appropriation as a risk factor is in Section 4.4.5. The analyses of the socio-political risk factors are the last two with foreign influence as a security risk factor in Section 4.4.6 and China as a risk factor in Section 4.4.7.

Each cultural risk factor analysis is linked to the literature review in Chapter 2 and the discussions in Chapter 5. These cultural risk factors are directly linked to security threats that may jeopardise the CS readiness of hospitals in Tonga.

The review of current literature in Chapter 2 demonstrates the role of humans as risk factors in CS socially, culturally, and politically. No similar studies are available on cultural risk factors in the context of Tonga or the Pacific. This research addresses this gap by investigating the Tongan culture and socio-political factors to identify the vulnerabilities that would threaten information security and CS of

the new digital HIS and ICT in Tonga's hospitals. The public and private sectors in Tonga would benefit from this research in terms of building the right security culture in organisations and making an effective policy and legislation that would cover the unique culture of Tonga. This analysis seeks to answer the research question raised on page 36.

Recognising that cultural factors are human factors is a risk to the CS of computer systems in hospitals and across the board in public and private sectors, leading to compromising data security and privacy. Previous studies reveal how diplomatic relations and economic ties can become a risk factor and a threat to CS and digital HIS. To be specific, there is evidence of abuse in socio-political and economic ties between states and companies committing cyber-attacks and security espionage, and it is ongoing worldwide. The research design in Chapter 3 guides this research to identify the human factors in Tongan culture and socio-political elements in Tonga's society to provide some answers to the research question.

4.2 Anonymous Sources

This section presents a list of anonymous sources who offer information regarding the research topic. Information is voluntarily given on the condition that sources remain anonymous.

AS1 A senior health professional with links to Government ministers and an excellent knowledge of the MoH and the ministry executives. AS1 has an excellent understanding of Tongan culture, organisational management, and government corruption.

AS2 An IT professional with Government role. This person has an excellent understanding of Tongan culture and the risks to ICT. Also well aware of corruption in Government.

AS3 In academia with links to Government ministers. Possess an excellent understanding of Tongan culture and organisational management. Is very well aware of the corruption in Government and current events in Tonga.

AS4 A health professional with ties to the MoH. Has links to Government ministers and knowledge of Government responsibilities. Possess an excellent knowledge of the MoH network and executive management. An excellent knowledge of Tongan culture and organisational management.

AS5 An IT professional with excellent knowledge of Tongan culture, organisational risks, and management. Excellent knowledge of eGovernment initiatives, current affairs, and corruption cases.

4.3 Acquiring Evidence

This section describes the process for the collection of data used in the study. The evidence obtained and used in this study is from past events and first-hand experience. The evidence is from articles, online video footage from local Tongan sources such as the Tonga Broadcasting Commission and Tongan Government, anonymous conversations, and years of real-life experience.

As far as one is aware, this research is the first on CS that considers cultural risks in a Tongan social context. There are previous studies on cyber threats to information systems in Tonga that include a technically focused study by Laulaupeaalu (2016), and discussion of legal issues for a CS framework for the Tongan Parliament by Lutui (2021). The study from Campean (2019) recognises cultural neglect as a human risk factor.

Evidence discovered is linked directly to the discussion of risk in Chapter 5, for example, there are cases of corruption, nepotism, and favouritism in the workplace that have been created by a culture of social privilege, social rank, and gender discrimination. The cultural tradition of tufakanga (division of labour) between genders leads to gender discrimination and gender appropriation, which causes unnecessary pressure in the workplace. Social oppression of women also leads to disadvantages for women in terms of acquiring the knowledge and skills required for ICT and CS. Socio-politically, the external influence of China is identified as a security threat with known cases of security espionage and crimes against foreign companies trying to enter China's market (see Section 5.2.7).

Due to restrictions on the availability of relevant individuals and data, there are findings and evidence that this research could not verify. The lack of data evidence from Tonga leads to the removal of a significant portion of information about violence and sexual abuse that may have links to data security. The recent findings from the Ministry of Internal Affairs in 2019 in Table 4.1 disclose that three in four women and girls (75%) in Tonga experience either physical violence or sexual abuse inflicted by a partner or another individual. Approximately two out of three women have experienced abuse since the age of fifteen, with teachers or fathers as the primary culprits. Approximately 47% of women chose not to disclose the abuse and violence endured. 75% of victims did not seek assistance from agencies or authorities. Over half of physical violence cases against women have children as witnesses. The survey results on children victims show that 40% experience nightmares, 18% have bed-wetting problems, and 37% deal with aggressive behaviour (Ma'a Fafine Tonga Inc, 2010). The reason why these data are significant is because women represent 51% of Tonga's population compared to men at 49% (Tonga Statistics Department, 2021). The proportion of men continues to fall as more men travel overseas for

work.

Gender	Population %	Figure	Explanation
Female	51%	75%	3 in 4 are victims
Female	-	47%	Choose not to disclose
Female	-	75%	Choose not to seek help from agencies or authority
Female	-	40%	Assault in front of children
Male	49%	-	Perpetrator identify as partner or unknown
Children	-	40%	Victims or witness, experience nightmare
Children	-	18%	Experience bed wetting
Children	-	37%	Deal with aggressive behaviour

Table 4.1: Data on violence and sexual abuse in Tonga- 2019 Report (Ma'a Fafine Tonga Inc, 2010)

The absence of employee-related data in the report suggests a lack of evidence regarding the occurrence of this issue in the workplace. Occasionally, news and social media highlight incidents of teachers engaging in physical abuse or instances of violence among students. However, there is currently a lack of information regarding such issues among employees. Ultimately, the critical aspect is the influence of cultural norms on workplace dynamics, wherein most personal matters are typically kept behind closed doors. Talking about sexual abuse and physical violence is considered taboo or shameful, leading many cases to go unreported. Victims are often encouraged to keep silent and make amends without involving the authority (Guttenbeil-Likiliki, 2008).

The cultural issues of violence and abuse pose a CS threat when it impacts the wider population. It is possible that some hospital staff, particularly women, are victims themselves but are hesitant or ashamed to report any incident. While incidents may occur outside of the hospital, victims as employees can harbour trauma at work, which can negatively impact employee performance, jeopardising the security of systems, the confidentiality of information, and the well-being of patients under hospital care. In the workplace, there are instances of employees suffering from mental breakdown and personal trauma that go unnoticed and unaddressed. Unfortunately, some cases are discovered too late, resulting in harm. This issue presents a significant challenge to Tonga, as victims are instructed to return home and reconcile rather than receive the necessary support and access to a secure environment for seeking refuge (Guttenbeil-Likiliki, 2008). If some hospital employees are silent victims, it becomes a liability to both patients and the security of the ICT. The well-being of hospital employees is essential in keeping the human factor in CS healthy.

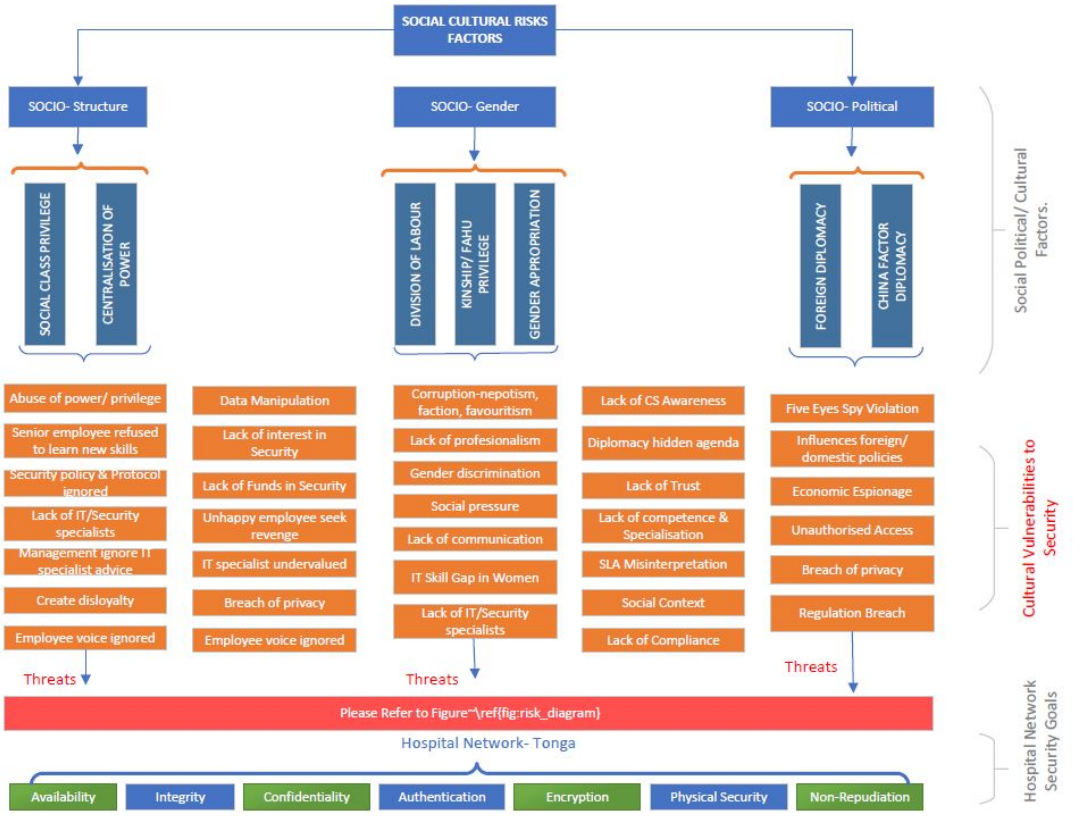

Figure 4.1: Tongan Cultural and Socio-political Risk Factors classified with security threat and areas of security affected.

4.4 Cultural Factors and Risk

This section analyses eight cultural risk factors identified as threats to the CS readiness of hospitals in Tonga (Figure 4.1). Five of the risk factors are cultural, two are socio-political risk factors, where one is an analysis of foreign influence in Tonga. The last analysis presents China's business activities in Tonga and the Pacific as a security risk factor. Each section has two parts of an analysis of each cultural and socio-political risk factor. The second part is the analysis of how these risk factors become a security threat to systems and information security in Tongan hospitals.

4.4.1 Cultural Risk Factor 1: Social Stratification and Social Class Privilege

The Commonwealth Education (2024) defines social stratification as the ranking of individuals in society according to a certain degree of importance through institutional social construction. Based on the societal value system, this importance also carries associated perceptions and values attitudes, such as race and ethnicity. Social stratification is a type of inequality that dates back to the hunter-gatherer period.

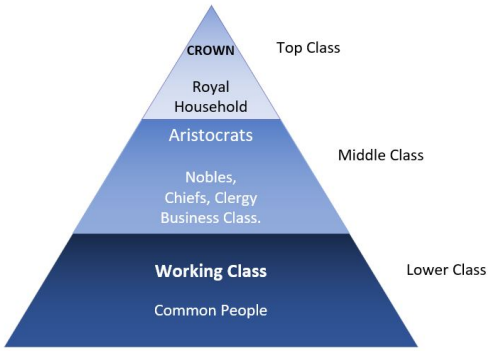

Figure 4.2: Tongan Class Society or Social Hierarchy

Hunters get status and prestige as awards based on its ability to meet these expectations. The expectation includes men being a superior hunter. Those who achieve superior expectations become highly-ranked figures in society. These rankings also draw influence, authority, and power. Since women are not hunters, their value comes from the responsibility to gather and reproduce.

In the Tongan context, social stratification also manifests in the ranks of high chiefs and monarchs. Rules date back as far as 950.AD. Social ranks at the top and middle class attract influence, power and riches to those born into aristocracy. Tongan social class consists of three levels (Figure 4.2) in which the top of Tonga's class society are the Crown and the royal household, the nobility and high chiefs in the middle, and commoners in the third class. Social status at each social level is hereditary, where royals and aristocrats maintain status and influence by marriage within the top and middle classes. A hierarchical society encompasses various aspects of individuals, titles, ha'a (tribes) and even different classes of dialects in the Tongan language, carrying different levels of importance to use in different classes (K. James, 1990). Chiefly title is organised according to rank and individuals who receive a title and subsequent generations from tribes known as ha'a (Kaeppler, 1971). These titles have symbolic and governmental importance. The knowledge of ha'a is predominantly limited to chiefs who seize advantage through power dynamics or adhere to traditional practices.

Bott (1981) discusses the emergence of a new middle class in modern Tonga since the 19th century, predominantly consisting of individuals with higher income, education, and occupation. In Tonga, wealth does not directly translate into social status or title. However, it can elevate commoners to the middle class, grant access to the governing elite, or enable marriage into the aristocracy (hou'eiki) or even the royal household (fale 'o e Tu'i) (Rubenfire, 2017).

In Tongan society, social stratification and class systems come with privilege that is deeply ingrained in Tongan social culture and tradition. Authority (mafai) and privilege (monu'ia) are closely intertwined

and are observed across various societal levels (K. James, 1992; Filihia, 2001). Having privilege and authority offers advantages and opportunities to those who possess it. Authority bestows benefits such as access to resources, connections, and information. For instance, royal family members and aristocrats enjoy greater privileges than commoners. The government and non-governmental organisations share similar hierarchical structures, where a system of authority is in place. Additionally, opportunity within organisations reflect these norms such that as one ascends in rank, one's level of authority and privilege increases. In religion, a comparable framework and hierarchical structure ensures smooth functioning, with higher-ranked individuals enjoying privileges.

Social Class Privilege Becomes a Security Threat

Privilege becomes an issue when abused by those who possess it. Social stratification as a form of inequality, as mentioned earlier, can be used positively to lead and keep order in society or the workplace. The same inequality can also create other behaviours of favouritism, nepotism, and factions, which have become a culture in Tongan society and the workplace. This culture usually starts at the top, where those with privilege exercise this behaviour to maintain influence and power in society and the workplace. This behaviour becomes a cultural artefact that creates an environment or breeding ground for corruption and an abuse of social privilege. Corruption may be expressed as preferential bias as employment positions are given to a person on the basis of social status, friendship, blood relatives, political factions and affiliation, favouritism and not on merit.

In relation to CS, class-based bias leads to unauthorised access or sharing of confidential information, resources, or access to a person of interest in the elite class for personal gain or malicious intent. Privilege awarded to the top and second class can use social status and privilege to achieve or access resources that the general public cannot. For example, Tongasat (Mendosa, 1994) and Shoreline Group (Trevett, 2006) demonstrate how royal privilege has led to the takeover of state assets while claiming the process as privatisation.

In hospitals, executives and employees maintain privileges to access digital HIS in the course of their work. However the potential to abuse user access privileges in HIS by healthcare employees does exist. Taking into account the social and cultural environment in Tonga, inappropriate access to records is common. The concept of a CS culture is new and widely misunderstood by both healthcare staff and the wider public. The MoH may have an advanced security mechanism in place, but human factors represent threat when staff do not exercise caution and security preservation at all times (Huang & Pearlson, 2019). Employees are the primary facilitators and enablers of cyberattacks in the health sector (Bassett et al.,

2021; Samy et al., 2010).

A corrupt culture can thrive in the workplace if leadership remains unchecked. The importance of having the right CS culture in an organisation highlights the significance of leadership as the creator of organisational culture in which CS is a sub-branch (see Section 2.4). By their actions, the leader as a role model influences the cognitive beliefs of employees (Huang & Pearlson, 2019) and those leaders who prioritise CS in everyday practice and engagement are shown to influence employee behaviour significantly. Having the right organisational CS culture is relevant to Tonga's MoH which is in the early stages of adopting digital technologies (see Section 5.2.1).

Favouritism (filimanako)

Favouritism is the act of giving unfair preferential treatment to one person or group at the expense of another (Oxford English Dictionary, 2024). Favouritism is linked to social class, stratification, and privilege and has existed since before Europeans arrived in Tonga. In modern Tonga, favouritism finds its way into the professional domain, both in the public and private sectors, which leads to corruption (Section 4.4.1). Members of the royal household and the aristocrats involved in the privatisation of public assets by utilising special privileges exploit opportunities via favouritism and nepotism. The privatisation of Tonga's state assets, including Tonga Power, Telecommunication, and Brewery, all included under the management of the Shoreline Group, were owned and operated by the former Crown Prince of Tonga-Tupouto'a (Trevett, 2006).

Tongasat, a private company, acquired Tonga's airspace rights and management in the 1980s and only exists because of royal privilege. Tongasat became a reality when HRH Princess Pilolevu obtained permission from King Tupou IV, which influenced the Tongan Government to approve rights to Tonga's airspace as a public asset (Mendosa, 1994). HRH Princess owns 40% shares and associates own the remaining shares. Tongasat suffered controversy and lengthy court battles, ending in bankruptcy. Shoreline Group suffered the same fate due to public pressure and was the victim of riots in Tonga's capital on November 16, 2006, (Trevett, 2006).

Nepotism (fakapone)

Nepotism (fakapone in Tongan) occurs among those with power or influence to favour relatives, friends, or associates, for example by offering jobs or opportunities for personal gain (Oxford English Dictionary, 2024). Nepotism in Tongan culture is a result of inequality, and is an expression of social stratification and social class. Traditionally, the privileges of land, title, and authority are inherited through bloodlines. This

social phenomenon creates the perfect environment for corruption through self-entitlement behaviour, favouritism, and factions to thrive at all levels of society.

The employment policy in Tonga is based on merit and favouring the most qualified individuals. However, there are reports of corruption where specific roles or positions are given to individuals based on social status and personal connection rather than merit, subverting the selection process. An example of nepotism is in the case of the political party founded by Tonga's former PM 'Akilisi Pohiva where his eldest son and son-in-law fought over the party leadership after the passing of Mr Pohiva. The Pohiva family made the headlines earlier over nepotism in which the former PM employed another son into the role of personal assistant (Radio NZ, 2008b). Since the founding of Tonga's modern Government in 1875, top Government offices are often reserves for aristocrats, the ruling class, or someone well-connected and influential. The PM role, for example, is often reserved only for members of the royal household and the aristocrats. The Crown selected the Privy Councils, the Cabinet ministers and the PM until King George V made changes in the late 2000s, allowing people to elect a Prime Minister to office, and Akilisi Pohiva was the first. Tongasat and Shoreline (Radio NZ, 2008a) cases are examples of nepotism and corruption where royal household members took over public assets from the Tongan Government through privatisation (Mendosa, 1994).

Factions (fakafahafaha'i)

Faction is defined as a small organised dissenting group within a larger body (Oxford English Dictionary, 2024). This phenomenon is very common in the social and political circle, which is often used to gain advantage, influence and power. Faction is very common in Tongan culture and society and in Parliament as well. Tonga's former PM Akilisi Pohiva is known as a champion of the pro-democracy movement that has fought against corruption in the Tongan Government since the 1980s. Pohiva is also the founder of Kele'a Media, a medium used to critique the Government's policies, deals and corruption and to amplify its pro-democracy doctrine.

Pohiva fought the Government for three decades and became PM in 2014 (Field, 2014; Tonga Parliament, 2014), and then the table turned (Vakauta, 2017). The Pohiva Government became the focus of criticism for nepotism, favouritism and conflicts of interest over Pohiva's link to the Pro-democracy party and the Kele'a Media (Vakauta, 2017). While Pohiva's family newspaper, Kele'a, benefits from Pohiva's transition to power, Pohiva also faces heavy criticism over the abuse of prime ministerial power (Hill, 2016). In Pohiva's defence, a statement was released as a reminder to Tonga Broadcasting Commission (TBC) of its primary role as a state owned media is to facilitate the Government work. TBC

contends that media freedom in Tonga should apply equally to all forms of media regardless. The link between corruption and risks to the security and privacy of information is discussed in Section 5.2.1.

4.4.2 Cultural Factor 2: e-Government Incentive and Centralisation Leadership

This section analyses the centralisation leadership as a cultural risk factor that poses security threats to the CS readiness of digital HIS at hospitals in Tonga. The new eGovernment move towards centralisation reflects the Government moving away from de-centralising leadership in Government agencies, channelling information, communications, decision making and power into a central hub under the care of the PMO and the Executives.

The Tongan Government's wishes to bridge distances between communities by expanding the deployment of e-Government, e-learning, e-commerce, and e-entertainment. To address this need, Petelo (2017) reveals the National ICT vision and strategies that can enable the Government and businesses to deliver critical services and bring communities closer together by utilising ICT to connect Tonga and the world. The initiative requires a physical extension of submarine fibre cable connecting the main island Tongatapu and the other main centres that is supported by upgraded microwave links (Figure 1.3). The extension of the availability of training and skills in modern ICT is expected to increase foreign investment in the field.

The new e-Government framework illustrated in Figure 1.2 provides a web portal to be used as a one-stop-shop for e-services and information. Tonga's e-Government solution promotes integration between the Government, citizens, and businesses where the web portal reduces the cost of manual work done in the old HIS. The portal is intended to produce high-quality work, eliminate redundancy in tasks across departments, and reduce labour costs. It is also the new e-Government incentive to minimise duplication and variation in e-Government systems and information.

Centralisation Becomes a Security Threat

CS risk in the centralisation of services and technologies leads to leadership, where decision making power accumulates. A risk factor is identified when managers make decisions without due consultation and centralisation leadership demonstrates one-way communication. Restricted communication is where employee feedback, opinions, and contributions in decision-making processes are not encouraged. Mr Kalafi Moala, a well-known pro-democracy media editor in Tonga, stated at a panel discussion at the Pacific Press Conference in Auckland in 2017, that no matter what political reform Tonga goes through and whoever is in charge, corruption will continue to prevail and that corruption is not dealt with (Pacific

Media Centre, 2017). A number of factors (Campos & Reich, 2019), including beneficiary, bureaucracy, and budget, affect the politics of policy implementation in the health sector, especially in developing nations (see Section 2.5.2).

Huang and Pearlson (2019) establish the significance of maintaining this connection between employees and those in leadership and CS culture (see Figure 2.2 and Section 2.5). Managerial leadership and culture reciprocate each other in a two-way relationship. This is between culture and employee behaviour, and managerial leadership and external forces shape CS culture.

The consequences of the breakdown between culture, employee behaviour, managerial leadership, and external forces contribute to unhappy, disloyal employees who may intentionally ignore security policy and protocols or even become cyber criminals out of revenge (Luna et al., 2016). Cybercriminal actions are deliberate, intending to cause damage (Giansanti & Monoscalco, 2021; Cybersecurity and Infrastructure Security Agency, 2021) by deploying ransomware, DoS attacks, or compromising medical devices (see Section 2.3.1).

Hospital HIS exposure to cyberattacks due to increased connectivity through the new e-Government network is a CS risk (Figure 1.2). While the global use of electronic health technology presents significant opportunities to improve clinical results and transform Tonga's healthcare delivery system, concerns about the safety of medical equipment and data are becoming obvious. Due to increasing connectivity to current computer networks, medical devices are vulnerable to new CS risks (Coventry & Branley, 2018). Healthcare is a prime target for cybercrime because of a lack of defences and the abundance of valuable data. CS breaches involve assaults on implanted medical devices, ransomware attacks on hospitals, and the theft of health information. The MoH network in Tonga (Figure 1.3) is digitally connected, alongside other agencies, to the e-Government web hub, exposing the entire MoH network to external cyberattacks (Huang et al., 2018) and internal users enabling cyberattacks that exploit vulnerabilities in the digital HIS.

HIS breaches can endanger lives, weaken health systems, and erode patient trust. Ultimately, patient safety depends on CS, but it has historically been inadequate. For this reason, CS needs to be a crucial component of patient safety. A comprehensive solution necessitates modifications to technology, procedures, and human behaviour. Cybersecurity and Infrastructure Security Agency (2023) emphasises the use and benefits of network segmentation to limit the spread of cyberattacks and minimise damages across hospital networks. This method also protects vulnerable devices within the hospital network that are not designed with advanced security defences from harmful traffic. The impact of a cyberattack on digital HIS is more harmful than any other sector (Luna et al., 2016; Bergal, 2022; S. J. Choi & Johnson,

2019; Cybersecurity and Infrastructure Security Agency, 2021) because of multiple damage to data security, disruption to service and delivery, and the lives of patients and employees (see Section 2.3.1).

Additionally, natural disasters like Tonga's proneness to earthquakes, volcanic eruptions, tsunamis, tropical cyclones and floods can cause significant damage to the e-Government network infrastructure. Damage can take a long time to repair, exposing the network to CS attacks.

4.4.3 Cultural Factor 3: Division of Labour Tradition (tufakanga)

This section analyses tufakanga, or the tradition of division of labour, as a cultural risk factor that poses security threats to CS readiness of digital HIS in hospitals in Tonga. Tufakanga is the segregation of roles based on gender which cannot be crossed and reflects the roles men and women play in society. Elders and the community at large frown upon anyone crossing the line or exchanging roles with the belief that it is unnatural and breaks tradition (Guttenbeil-Likiliki, 2008; Bott, 1981; Runeborg, 1980).

Helu (1995) describes the history of this tradition, that the roles of men have undergone significant change in response to economic and social reorganisation throughout Tonga's history. The role of men in ancient Tonga is bound to the service of defence and war services (taumalu'i fonua), voyaging (fai folau), and deep sea fishing (toutai loloto). Women are left with household affairs, including cooking (fei me'atokoni), gardening, reef fishing (fangota), and house furnishing. The arrival of Christianity in the late 19th century and the unification of Tonga under one rule brought a period of peace. This social realignment liberated men to adopt the modern division of labour that focuses on agriculture, heavy work includes construction, canoe building, heavy gardening, and earth-oven cooking (fei'umu). In this reorganisation, women become primary producers of koloa (the production of fine mats and tapa) in addition to general housework, child rearing (tauhi fanau), daily cooking, and cleaning. Koloa are vital to Tongan society and are used in exchange for gifts or goods.

Despite social changes and economic demands, the primary role of men in Tongan society is to provide and protect (Guttenbeil-Likiliki, 2008; Bott, 1981; Runeborg, 1980). The highest male role in Tongan society is to lead, either as king, chiefly title, church leader, leading position in Government, Parliament or simply the head of a kainga as 'ulumotu'a or head of the family. However the home will always belong to women, hence the Tongan saying ko e 'api 'a fafine that translates as the home that belongs to women and that provides some degree of power to the role of women in Tongan society. This differs from the English saying that a woman's place is in the home or kitchen, which is degrading and disrespectful (ta'e faka'apa'apa).

In Tonga today, some of these roles cross over due to education, religion, technology, and foreign

influence (Helu, 1995). For example, 22.1% of households are now headed by women (United Nation Women, 2022). This percentage continues to rise with more men leaving Tonga through seasonal worker schemes, studying abroad, or emigration. Both men and women may now take up office or other roles that are created through economic development. Despite changes in traditional gender roles, Tonga is still behind in women's rights and gender equality in employment, exposing areas traditionally dominated by men like ICT and CS (see Section 4.4.5).

Most staff in Tongan hospitals are women, employed as nurses and doctors but with limited skills in computer technology or CS (United Nation Women, 2022). Women are encouraged to remain in jobs appropriate for women, such as those in healthcare, teaching, hospitality, administration, customer service, and producers of koloa. Men are encouraged to continue being the provider and protector (Helu, 1995) with jobs in building, engineering, security and technology-related roles. Therefore, society believes ICT and CS are the responsibility of men because of its security and technical nature.

The division of labour tradition is seen as anachronistic and plays a conservative role, preventing development (Helu, 1995). The tradition of tufakanga in modern employment perpetuates the idea that women should only play women's roles and should apply to the workplace as well.

Division of Labour Becomes a Security Threat

The security risk of the tufakanga tradition is the prevention of the attainment of ICT and CS skills in Tonga. Fewer ICT and CS experts creates the potential for issues that become threats to CS readiness in digital HIS in Tongan hospitals.

The risk of building the wrong organisational and CS culture in hospitals is likely when there is a lack of ICT and CS experts (Huang & Pearlson, 2019). The importance of building the right CS culture in organisations and hospitals requires expert knowledge of ICT in leadership or executive roles as leaders build cultures in organisations (see Section 2.4). The e-Government and the digital HIS are in the early stages, therefore it is important that the right organisational and CS culture for the MoH and other Government agencies in the e-Government network are established.

Employees and management must understand that securing organisational CS depends on in-role and extra-role CS practices (Bhuyan et al., 2020). Employees must understand the significance of being in-role by behaving the right way at work, adhering to security policy and following protocols, and being responsible for reducing user abuse of computers (see Section 2.5.4). Employees must also understand the importance of the extra-role of CS practice within and outside the workplace by spreading CS awareness amongst health workers, helping co-workers understand this new culture and practicing good CS safety

for others to follow.

Failing to establish the right CS culture and raise awareness of in-role and extra-role CS among health staff in the hospital can jeopardise the CS of the entire digital HIS and ICT at MoH. The same cultural issues can also impact the rest of the e-Government network in a successful cyberattack. Common attacks are via ransomware and DoS (Cybersecurity and Infrastructure Security Agency, 2021), where the attackers aim to disrupt HIS and network services. The threats of tufakanga to CS and information security are further discussed in Section 4.4.5.

4.4.4 Cultural Factor 4: Kainga (blood relatives) Privilege

This section analyses the cultural concept of kainga (blood relatives) privilege as a cultural risk factor. This concept refers to blood relations, including the idea of kinship, fahu and veitapui within the kainga, and defines how people are related. This section focuses on these relationships as risk factors that can lead to corruption and nepotism, threatening organisational CS. The kainga shows how people are related to one another through ha'a (tribe) or marriage (Runeborg, 1980; K. James, 1990). Nofo 'a kainga describes how Tongans live as kainga in the community where there is expectation for (feveitokai'aki) mutual respect and care for one another (tauhi va) which maintains peace and order in the community (Bott, 1981).

Kainga often do favours or present gifts as a gesture of goodwill and appreciation (fetauhi'aki), but this cultural practice can be mistaken for a bribe. It is a common practice in Tonga to bear gifts in return for favours or appreciation for accomplishments or occasions. This practice can be tricky in the work environment when there are hidden agendas to return favours or to get something (Radio New Zealand, 2024).

In the concept of kinship, the Tongan family is a hierarchical structure where a father figure holds authority over managing the family, land, resources, and information (Rubenfire, 2017). According to Bott (1981), the Tongan kinship system is domestic and political. It consists of the most basic form of social hierarchy (Runeborg, 1980; K. James, 1990), which involves a structure where authority passes down through male lines and ceremonial rank is recognised. In the family circle, older siblings rank higher than the younger ones and the oldest male in the family is automatically entitled to inherit land, titles on the paternal side or family land. A man can also take on the title of tribe leader (ulumotu'a).

Fahu is the female superior figure in the family, the father's sister (mehikitanga). Women cannot inherit land and titles but can hold the fahu ceremonial rank and privilege that is significant in Tongan families. Women in the matrilineal kinship system may exert influence over patrilineal counterparts

(Rogers, 1975). Every male generation is subject to the privilege and influence of a patriline sister, and this privilege is passed down through a fahu lineage. A fahu has the authority to control brothers in rituals and hold honorific positions at special occasions. Helu (1995) clarifies that these mystical powers are mere effects and not the source, as the power of women flows from women's essential role in the scheming of things.

Bott (1981) clarifies that while fathers and sisters both receive respect, the reasons behind the respect differ. A father holds the authority to give orders and control resources, while his sisters can request a portion of the brother's produce. A fahu holds a position of honour and receives gifts during the ceremony as a mark of respect. A fahu is given a prominent seat at the forefront of the event (K. James, 1992; Filihia, 2001; Bott, 1981; Rogers, 1975; Runeborg, 1980).

Kainga (Blood relatives) Privilege Becomes a Security Threat

The risks identified in this section are via the privilege, influence, and social connection a person or group possess through the cultural concepts of kainga, kinship, and fahu, privilege. These cultural factors can be utilised in the same way as social class privilege in Section 4.4.1. The privileges derive from blood connections, privilege, and the influence of kainga, fahu, and kinship can significantly impact organisational and CS culture by relaxing the formality of routine and culture in organisations or hospitals because of these social and cultural relations. It is very common for relatives to work together in Tonga due to its small population. Additionally, the threat to CS emerges with the culture of casualised attitudes towards CS in-role and extra-role behaviour (Bhuyan et al., 2020), by abusing work computers and ignoring security policies and protocols (see Section 2.5.4) and learning bad habits from other staff (see Section 2.5.2).

The ability to affect other employees through group norms or culture presents a CS threat (Huang & Pearlson, 2019). Group norms play an essential role in forming an employee's attitudes, values and beliefs in the workplace. If the organisation's culture practices bad CS habits, other employees, including new recruits, would likely do the same and adopt a bad CS culture. However, executives in CS-aware organisations value cyber resilience when staff participate in CS discussions and activities, as it boosts CS awareness among staff.

4.4.5 Cultural Factor 5: Gender appropriation and career choice

This section is an analysis of gender appropriation as a cultural risk factor towards the CS readiness of hospitals in Tonga. Gender appropriation is the adoption of tradition or behaviour belonging to a culture

or social group in a way that is stereotypical, disrespectful, and exploitative (Britannica, 2024). Gender appropriation in the Tongan context is related to Section 4.4.3 where there is an expectation that men and women will follow tradition and choose education and career pathways appropriate to their gender. Gender appropriation is a cultural pressure that influences every aspect of life at all levels of society. It affects Tongan's perceptions of education, career choices, and the roles of women and men, personally and professionally. This research identifies issues in gender appropriation, for example, women are deterred from independently choosing education and a career path.

There is no law in Tonga to prevent women from pursuing an education or a career in any field. There is a general guarantee of equality under Tonga's 1875 Constitution Amendments, which states that the law shall apply to all people regardless of class (Guttenbeil-Likiliki, 2008). However, discrimination on the basis of gender, sexual orientation, gender identity, expression, and sex characteristics is not expressly forbidden under the Government of Tonga (2016) Constitution.

Tonga is known to have one of the highest numbers of PhD recipients per capita (University of the South Pacific, 2018) and Tonga's literacy from the age of 15 in men is 99.34% and women at 99.43% (Commonwealth of Learning, 2014; Japan International Cooperation Agency, 2010). However, many women who graduate with tertiary qualifications marry and retire at home, looking after the family instead of using those skills (Japan International Cooperation Agency, 2010; Guttenbeil-Likiliki, 2008).

Cultural pressure creates a gender gap that contributes to a lack of skilled professionals in CS and ICT. Tonga's MoH reflects a culture of gender appropriation in Tonga (WHO, 2015). As shown in Table 4.2, women make up 70% with only 31.6% that are specialist medical practitioners. Almost 50% of General Practitioners and 100% of midwives and advanced practice nurses are female. The proportion shows a high risk with women as a vulnerable group because, as described by AS1, AS2, and AS4, these health professionals have little to no knowledge or skill in ICT, on the new digital system, or how to work online safely without compromising security. Furthermore, US Govt Report (2021) on human rights in Tonga confirms employment discrimination against women and that pay gap differences occur.

Role	**Percentage**	**Gender**
Hospital staff	70%	Female
Specialised Med. Practitioner	31.6%	Female
General Practitioners	48%	Female
Midwifery	100%	Female
Advance Practice Nurse	100%	Female

Table 4.2: Percentage of Women in Healthcare-Tonga (WHO, 2015)

In addition, gender appropriation leads to gender discrimination in ICT and CS-related jobs. AS2,

AS3, and AS5 report that males prefer to work alongside male colleagues in ICT for cultural reasons, specifically in relation to veitapui traditions, the cultural belief of tufakanga holding with the traditional view that women do not belong in ICT and CS. ICT and CS come under the career categories of technical and security, and roles from a Tongan perspective these come within the male domain alongside engineering, architecture, and mechanics. AS1, AS2, AS3 and AS5 support the view that the reluctance of women to join the tech industry is directly related to culture and its perception of men and women.

Gender appropriation sets the tone for what is proper for men and women to do, think, and how to behave. A number of institutional and cultural factors, such as the nine Parliamentary seats reserved for male nobles, the dominance of men in unofficial government structures that prevent women from entering the political sphere (US Govt Report, 2021), and societal perceptions of women's appropriate roles and competence, discourage women from entering the field of politics. In 2021, only 1 out of 27 parliamentary seats are occupied by a woman, and 12 out of the 75 candidates of the November 2021 election are women (United Nation Women, 2022). Guttenbeil-Likiliki (2008) say that many view Parliament as a category reserved for men and is not appropriate for women because of the aggressiveness of men. Guttenbeil-Likiliki adds that Tongan women view being loud, talkative, and pushy as a sign of unfeminine behaviour that is excessively aggressive.

Gender Appropriation Becomes a Security Threat

The security threat identified is the lack of qualified ICT and CS experts in Tonga today. There is a small community of IT experts in Tonga, the majority of whom are men. The shortage of IT experts creates a demand for ICT and CS specialists, making the value of CS and IT specialists expensive. The lack of CS specialists and IT professionals is a direct threat to security in the workplace. Government agencies and hospitals need IT experts at the executive level to create the right CS culture in the organisation (see Section 2.4). Having the right people in leadership is vital for developing the right CS culture (Huang & Pearlson, 2019), they allocate resources and mechanisms to protect hospitals and organisations from cyberattacks and external influence. These executives are the role models influencing employees' in-role and extra-role behaviour in and out of hospitals.

There are reports of gender discrimination against women in ICT, and AS1, AS2, AS3, AS4 and AS5 all agree that the majority are males who prefer to work alongside male colleagues. Few women are employed in ICT and find it difficult to climb the corporate ladder due to gender discrimination, they are perceived as inferior and settle for other administrative roles. United Nation Women (2022) reports that 39% of senior roles (CEO,COO,CFO) in Tonga are taken by women. AS1, AS2 and AS3 report the

existence of toxic behaviour in organisations where women compete with other women because they do not want female colleagues to enter leadership roles or do not want to see women succeed. This toxic behaviour creates inside threats as unhappy staff who turn vengeful or as internal facilitators of cyberattacks (Giansanti & Monoscalco, 2021). Section 2.3.1 describes the objectives of threat actors; to disrupt services and cause maximum damage (Cybersecurity and Infrastructure Security Agency, 2021).

4.4.6 Socio-Political Factor 1: Foreign influences in Tonga

This section analyses foreign influences (diplomacy) as a risk factor for CS of digital HIS at hospitals in Tonga. Foreign influence and motivations are political and economic, affecting business information and communication security and risking CS across Tonga's networks, including hospitals. The research discovers that diplomacy enables activities in two areas that would compromise CS directly in Tonga and around the Pacific. These areas directly impact Tonga's foreign and domestic policy, where private and international entities' agendas impact Tonga and the Pacific. Section 2.5.2 reveals that interest groups and external factors do influence the politics of policy implementation in the health sector, particularly in developing countries that are vulnerable compared to developed nations which are strong economically and politically (Campos & Reich, 2019).

Five Eyes Alliance Spy Activities in the Pacific

Identification of hidden agendas of states and private entities exposes key players with interests and influence in the Pacific, including New Zealand, Australia, China, Britain, France, the United States, World Bank, WHO, and intelligence agencies like the Five Eyes Alliance. For many years, China has taken the blame for security breaches and spy activities worldwide, but recently it has become clear that Western Allies are spying around the Pacific, for example New Zealand's Government Communications Security Bureau (GCSB).

The media exposure of New Zealand's GCSB and the Five Eyes Alliance activities in the Pacific region includes the GCSB hosting of a foreign capability system that shares intelligence and technology with Australia, the US, and the UK (Fuatai, 2024). The GCSB is responsible for capturing signals intelligence transmitted by satellites and undersea cables from South Pacific countries; Tonga, Fiji, Vanuatu, Cook Islands, Kiribati and Samoa. The report reveals that all communication from all the Pacific countries' networks are scanned. Specialised computers filter data for specific keywords, phone numbers, and relevant metadata, such as location. Investigation reveals that foreign agencies controlled the spy system within GCSB between 2013 and 2020 without supervision. GCSB, in its defence, denies

any knowledge of the purpose of this intelligent system.

Considering the role of the GCSB in the Five Eyes Alliance, it allows foreign partners to carry out secretive and exploitation activities in the South Pacific region without informing Pacific states of what is happening. The New Zealand Parliament and the minister responsible also deny knowledge of these activities. Details regarding the spy system remain classified according to the report, but what is clear is that the intelligent system is used to process communications and identify remote targets. The technology is also linked to a top-secret US system in the capture-kill operation (Fuatai, 2024).

Fuatai (2024) also mentions the possibility for New Zealand to join the AUKUS, a military technology-sharing agreement designed to contain China. The AUKUS members are Australia, the UK and the US, who recently ran an operation of military systems using surveillance drones to feed AI-powered software for remote targeting by missiles. These systems utilise advanced technological communication systems to achieve immediate military results. The process is described as freely flowing data from sensors to deciders and through to effectors. According to Fuatai (2024), these effectors may be autonomous, a weapon system or even nuclear.

Foreign Manipulation of Tonga's Foreign and Domestic Policies

An analysis of risk factors based on how foreign diplomacy influences Tonga's foreign and domestic policies and how this becomes a security threat to Tonga's hospital's new digital HIS and CS readiness. Foreign diplomacy influences Tonga in many ways, from manipulating foreign and domestic policies and legislation to pressure to comply with the global agenda and peer pressure to take sides or join factions. Foreign donors send aid to Tonga under certain conditions, such as the requirement for Tonga to alter its foreign and domestic policies to align with the aid donor's objectives.

A global shift toward the adoption of digital health systems is led by the WHO and presented in Section 4.4.2. The Tongan Government policy on health is aligned with the WHO objectives with a guarantee of support from the WHO. The risk identified in Tonga's MoH joining the global health system includes the connection to external networks. The MoH digitalisation of 10 years of patient data from the hospital health archive and its upload to the new digital HIS is purported to be uploaded to G-Cloud. In addition, human factors present a threat, such as CS knowledge held by the executive and experts and the CS culture in the organisation, users of the digital HIS, attitudes to CS policy and protocols, and the level of security awareness.

4.4.7 Socio-Political Factor 2: Tonga-China Diplomatic Relations

This section presents an analysis of Tonga-China diplomatic relations as a security risk factor that this research identifies as a security threat towards the CS readiness of the new digital HIS in Tonga hospitals. China is a security risk factor due to the extensive evidence against the Chinese Government's involvement in illegal cyber activities against foreign businesses trying to enter China's market. Due to security concerns, China's illegal activities resulted in bans for Huawei technology around the world, as well as China-made devices from Government facilities across the United States, Australia, and Britain. The issue is that the Tonga Government continues to use these technologies in Government facilities and the Government Data warehouse, ignoring security risks. The other reason is Tonga's current position as a debtor to China puts Tonga at risk of being exploited and manipulated through policies and trade agreements and even silence from criticising China over issues on human rights and illegal cyber activities.

Tonga established diplomatic ties with the PRC on November 2, 1998, to join the United Nations (Fonua, 1998). China, in return, lavishes Tonga with gifts of monetary funds, infrastructures, computers and communication equipment. The St George Palace in Nuku'alofa is an example of China's gifts with a price tag of TP$25 million (NZ$18 million). The Prime Minister's Office, Foreign Affairs, and Treasury (until the end of 2023) are all housed at the St George building. China provided brand-new structures for Tonga High School, the country's top secondary institution, complete with computer equipment, in early 2000 (Aid Data, 2017; Fonua, 2003). Tonga's digital upgrade for the hospitals is funded by the Asia Development Bank and Tongan Government (Asian Development Bank, 2019). China tech giant Huawei facilitates the Government data warehouse. China granted USD50 million in loan money to the Tongan Government to rebuild its capital in 2018 (World Bank Organisation, 2016), and another USD45 million is again grant for road and infrastructure upgrade (World Bank Organisation, 2016). Both projects were completed in 2017, and repayment continues (Perry, 2019).

China a Security Risk Factor

A significant risk factor is Tonga's large financial and social debt to China, which puts Tonga in a challenging position if it were to refuse any demand from the Chinese Government. Tonga is losing its liberty to make decisions that may affect its diplomatic relationship with China. For example, Tonga must declare Taiwan as part of Mainland China. Tonga must not join other countries in challenging or criticising China's dealings. In Tonga's case, the Chinese Communist Party (CCP) explicitly declares

that the loan to Tonga holds no political conditions and that the debt negotiations are handled smoothly and peacefully. However, the repercussions of Tonga publicly denouncing China's humanitarian crimes and illegal agreements are uncertain and can only be determined over time. Tonga's outstanding debt presently amounts to $195 million, accounting for 35.9% of its GDP.

In addition, China's reputation for illegal cyber activities worldwide is evidenced in reports and data. In 2018, the Trump Administration conducted a thorough investigation under US Section 301 of the Trade Act of 1974, which led to the revelation of China's illicit activities (Office of the United States Trade Representative, 2018; White House Office of Trade and Manufacturing Policy, 2018). The investigation reveals that the Chinese Government supports and conducts cyber intrusions targeting confidential business information that belongs to US firms. Trade secrets, negotiating positions, technical data, and private and confidential internal communications are among the economically important sources of information that the Chinese government successfully obtains.The research also finds that the Chinese government uses cyber intrusion to further its strategic economic goals and that these goals are closely related to China's industrial strategy.

The US investigation also revealed a report by the CS firm Mandiant in 2013 presenting China as the world's most active industrial and state espionage actor at 95% (Office of the United States Trade Representative, 2018). The report also exposes the involvement of the People's Liberation Army (PLA) General Staff Department and the Third Department (3PLA) in the theft of hundreds of terabytes of data. Details reveal that at least 141 organisations are victims of data theft, where 115 are US-based. These victim entities represent 20 of the major industries in Figure 4.3.

International Community Respond to China

Nations and organisations are addressing the issue of China's CS abuses and criminal activities through discussion and legal actions, although the outcomes are generally unproductive (Office of the United States Trade Representative, 2018). However, the concern over security breaches and potential espionage by the Chinese Government through Chinese tech companies like Huawei and China-made devices by Hikvision and Dahua are of concern (White House Office of Trade and Manufacturing Policy, 2018). The US Government sanctions against Huawei in 2019 are in response to the connection with the Chinese government (Aljazeera, 2018). The sanction resulted in the phasing out of Huawei's mobile phones and the loss of contracts worldwide (Reuters, 2023). In 2022, the US banned Chinese-manufactured CCTV cameras, intercoms, electronic entry systems, and video recorders from all government buildings. The ban is directed at the Chinese state-owned companies and Hikvision brand, which follow the security

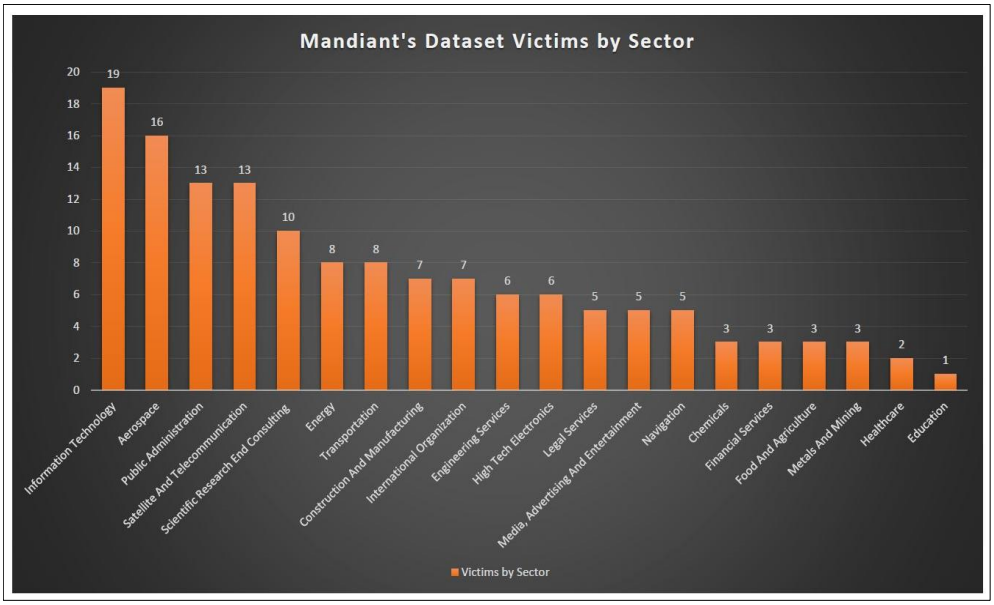

Figure 4.3: Exposing one of China's cyber espionage unit (Office of the United States Trade Representative, 2018)

laws of the People's Republic of China (The Verge, 2022).

UK and Australia followed the measures above by implementing a similar ban on Chinese-manufacture intercom systems and surveillance cameras (Australian Institute of Internal Affairs, 2023; W. James, 2022). The ban ordered the removal of devices from the offices of nearly one hundred federal politicians in Australia. A thorough review by the Australian government identifies a minimum of 913 devices operating in government departments and agencies, including the Defence Department and Ministry of Foreign Affairs and Trade (Reuters, 2023; Dobberstein, 2023).

On the other hand, New Zealand's membership of the Five Eyes Alliance faces criticism from fellow members for not condemning China's actions and violation of human rights (McClure, 2021). The New Zealand government is careful when criticising China due to concerns over jeopardising trade relationships. Since China accounts for more than 29% of the country's trade and is New Zealand's largest trade partner (NZ Foreign Affairs & Trade, 2022), the government is exercising caution in this matter. China primarily uses trade to demonstrate its dissatisfaction and impose consequences on individuals who have the audacity to criticise the Chinese Government (Manch, 2021).

4.5 Conclusion

This chapter reports on findings in this research, including extensive materials, years of personal observation, and rich knowledge of Tongan culture, identifying the risks relevant to the security and privacy of data and digital HIS in hospitals. The research identifies five cultural and socio-political risk factors in Tongan society that threaten CS of digital HIS in Tonga's hospitals.

The discussion of how these identified risks become a security threat and how these risk factors can cause breaches to security in hospital data and digital HIS are discussed in detail in Chapter 5.

Chapter 5

Discussion

5.1 Introduction

Chapter 4 presents the findings gathered from sources during this research. These findings are obtained from applying the method in Chapter 3. Findings from relevant literature, documents from the Government of Tonga, official surveys published in Tonga, international and Tongan media, personal knowledge and experience of growing up in Tonga. This chapter addresses the research question on page 37 and discusses the findings and how each cultural factor is a security threat to CS of digital HIS in Tongan hospitals. The discussion also links back to literature on CS threats and attacks faced by the healthcare industry worldwide and the importance of protecting digital HIS in hospitals (Chapter 2).

The aftermath of a cyberattack in a hospital cannot compare with any other sector because of the extensive damage and immediate impact on service delivery, as well as the lives of patients and staff. The discussion presents the significance of building the right culture in the organisation, starting with the executive level.

5.2 Cultural Risk Factors Becomes a Security Threat

This section discusses five of the cultural risk factors discovered during this study (Figure 5.1). The first three Risk Factors are sourced or related to Tonga's social stratification and social class hierarchy, where privilege originates. Risk Factor 1 discusses social stratification as a form of social inequality and the privilege that comes with it. Risk Factor 2 presents the centralisation of structure, leadership and network in Tonga's new eGovernment incentive as a cultural risk factor, and Risk Factor 3 is the division of labour.

Figure 5.1: The Cultural and Socio-Political Risk Factors and associated Security Threats

Risk Factor 4 is the cultural concept of kainga (blood relatives), kinship and fahu privilege, and Risk Factor 5 is the cultural risk of gender appropriation. The last two risk factors are socio-political risk factors from foreign influences and from China.

5.2.1 Risk Factor 1: Social Stratification and Social Class

This section discusses the CS threat of social stratification and social class towards digital HIS and the CS readiness of Tongan hospitals. As discussed in Section 4.4.1, social stratification is a form of inequality that confers social rank and privilege to those who inherit power in the top and middle class and executive positions (Figure 4.2). Social privilege creates a culture of favouritism (Section 4.4.1), nepotism (Section 4.4.1) and factions (Section 4.4.1) which identifies as corruption behaviours and are a threat to CS in Tonga's hospitals. Common types of corruption in healthcare worldwide are nepotism, favouritism, data manipulation, embezzlement, recruitment fraud, bribery, conflict of interest, regulatory capture, state capture and procurement corruption (Health Policy Watch, 2023).

In Tongan society and culture, anyone with privilege can get opportunities and access to many

things, places, and people that an ordinary person from the working class could never get. In society, an aristocrat with privilege commands respect, obedience and loyalty from others. The power of privilege makes its way to organisations or the workplace. Whether it is people in management or aristocrats at work, privilege works the same. That privilege gives people access to what they need, such as money, information, resources or services through the proper process or special privilege. In Tonga, access to resources and information comes from who a person knows rather than what a person knows. Nobody can establish much or go further in business without the help of the aristocracy. Shoreline Group (Radio NZ, 2008a; Scoop Media, 2006) and Tongasat (Mendosa, 1994) are two examples of how privilege at the highest level of society can get access to people, information, place, position and business opportunities based on social rank, power and privilege.

Enabling and empowering a culture of corruption in hospitals and across Government agencies (Figures 4.1 and 5.1), social stratification creates social privilege along with other social behaviours of favouritism, nepotism, and factions (Section 4.4.1). The link between corruption and cybercrime is discussed in (Jordan, 2023). Hospitals face a multitude of internal and external cyber threats. While internal threats are often attributed to negligence, external threat actors increasingly target internal staff members, particularly those in trusted IT and security positions. These threat actors may use corruption to exploit vulnerabilities in even the most advanced cyber security systems. Many cybercrime groups operate as organised crime syndicates, willing to resort to corruption to achieve the group's objectives.

In hospitals, health employees have user privilege to log in and access the digital HIS and patient health information. A user privilege can access limited confidential patient information, whether it is for a case they are directly involved with or for other intentions. However, a user can access confidential patient information and share it with others without permission or the patient's consent. An outsider with social privilege can use that authority to influence an employee in the hospital to share confidential information without permission. This breaches employee-patient confidentiality and the patient's right to privacy and security.

Currently, the law in Tonga and security policies in hospitals do not protect data or stop employees from breaching security protocols, nor are there consequences for those who commit these breaches. Legislation similar to the HIPAA in the US healthcare sector proves effective in healthcare facilities' everyday operations (Langer, 2016; Swede et al., 2019). HIPAA is a US Federal law and is mandated in every US state. This law requires all hospitals and healthcare facilities to install and run software that tracks all user activities accessing patient health information. Every employee is required to comply, which protects patient health information and ensures privacy from unauthorised access and disclosure

of information without the patient's consent. The software flags and tracks all employee's log-ins and all patient searches. The consequences of unauthorised access are disciplinary action, loss of job, or litigation and fines.

Therefore, regular training for staff and users of systems in hospitals is essential to raise CS awareness. Tonga needs legislation similar to HIPAA and staff regular training starting that includes top management is required to develop a CS culture in the organisation. Consequences for security breaches must be exercised through internal disciplinary action or law enforcement for the security policy to be effective.

5.2.2 Risk Factor 2: e-Government Incentives and Centralisation of Information and Control

This section discusses the security threat of centralisation management and leadership to digital HIS, data security, and privacy in Tonga. Referencing Section 4.4.2 and the Tongan Government's vision for the new eGovernment framework in Figure 1.2, this study focuses on identifying potential security risks and threats.

Traditionally, centralisation management and leadership weaknesses are enabled through staff vulnerability to corruption. Centralisation is vulnerable to corruption, where the accumulation of power at the top may lead to authoritarian leadership. The security threat is the impact of authoritarianism on hospital staff and workplace culture and how that becomes a security threat to digital HIS and data security. A group or individual with too much power is vulnerable to corruption (Table 2.1). AS1, AS2, AS3, AS4, AS5 (Section 4.2) reports that those in power can choose to grant, remove, manipulate, or withhold access to data and information to suit their agenda or to maintain a position of power. Additionally, they report that authoritarian leadership discourages creativity and a sense of ownership that slowly erodes over time. Staff's sense of motivation and morals are also affected, resulting in a decline in performance.

It is the responsibility of leadership to establish a CS culture (Schein, 1996). CS culture in Tonga is at an early stage of development and leadership needs to start building the right CS culture at MoH. Possessing the right skills to effectively handle and nurture that culture is vital in developing the right CS environment (Marotta & Pearlson, 2019) through the evaluation of long-term objectives, internal hierarchy, managerial decisions and conduct, and the behaviour of staff.

According to AS1, AS2, AS3, and AS5 (Section 4.2), a lack of communication between top management and staff in the organisation becomes a threat that could lead to a number of outcomes with devastating consequences. In a class-based society, the elite do not mix or socialise with ordinary people and similar attitudes prevail in the workplace, creating a rift between management and staff. A common

example are leaders that make decisions impacting CS in hospitals without input from staff and CS experts. This ignorant behaviour can lead to loss of loyalty and adopting rebellious behaviour (Giansanti & Monoscalco, 2021). A toxic workplace culture and unhappy work environment may be a breeding ground for insider threats with unhappy employees seeking revenge, with a willingness to provide access for hackers and threat actors to organisational systems or to sell company information (Section 2.3.2).

Other issues linked to CS risks and threats to CS readiness develop into a lack of transparency, procurement corruption, embezzlement, conflicts of interest, and bribery (Health Policy Watch, 2023). Holovkin, Tavolzhanskyi and Lysodyed (2021) points out that CS cannot survive in a corrupt environment that fails to prioritise information security.

The study reveals that management typically overlooks the funding required for hospital IT and security. While executives may have become aware of the importance of IT and CS in healthcare, the lack of funding in hospitals results in outdated systems and equipment, exposing the new digital HIS to cyberattacks. The hospitals in Tonga still use computer equipment that is outdated, including some computers that still operate on Windows NT 7 (Ministry of Health Tonga, 2019). This is the same version that was used in the attack at Waikato DHB when cybercriminals successfully hacked into the DHB's 600-plus servers in May 2021. Investigations identified that hackers can infiltrate systems months before the actual attack, which affected hospital staff and patients. The delay in bringing the systems back up caused chaos for everyone involved, with service delays, cancelled appointments, and operations being transferred out of Waikato. Subsequent stolen data saw 4200 patient information leaks into the dark web (Yeoman, 2021). This attack breached security in all levels. Therefore it must be noted that IT security not only protects the digital HIS systems, maintains the confidentiality and integrity of hospital data. IT security also secures the smooth and continuous operations of hospitals as well as maintains the functions of medical devices.

AS2 (Section 4.2) addresses the threat of hospital staff not accepting the new digital HIS. Also, AS2, AS4 and AS5 (Section 4.2) emphasise that maintaining security awareness and tech support among healthcare staff is required so that staff keep up with security policy and adhere to security protocols. A lack of communication between executives and staff and the lack of support from IT professionals increase the likelihood that staff will not adopt new technology and disregard security protocols and measures (Holovkin et al., 2021). The issues raised by AS2 (Section 4.2) point to the comprehensive misunderstanding of digital technology, lack of tech skills and awareness by general healthcare staff, an apparent generation gap with senior staff, and old habits from the manual HIS. Technology acceptance takes time, and senior staff's reluctance to learn and assimilate to new digital HIS and security protocols

is a risk to systems and data privacy (Health Policy Watch, 2023). Despite having a strong and secure security system, weak human factors can lead to breaches of security due to a lack of training and awareness. An employee with no security knowledge and experience of risks will not be able to tell the difference between genuine and threat emails and what to do to verify them. As a result, untrained staff could click on links, opening the door to threats leading to unauthorised access to hospital systems (Section 2.3.1).

The technical danger of centralisation in the event of a successful cyberattack on the Government portal framework is illustrated in Figure 1.2. Tonga's Government agency systems, citizens, and specific businesses are connected to the Government portal, and information is shared between relevant agencies (Ministry of Health Tonga, 2019). For example, the hospital system shares birth and death records with the Government Registration Office that issues certificates of birth, marriage, and death. All agencies share information with Statistics, Treasury and Audit Department and other Government businesses. Any successful attack on the Government Hub will harm the entire digital network (Huang et al., 2018) as well as critical infrastrctures at the national level. Detection of a successful attack may take months to be confirmed, either by an external entity trying to help or cybercriminals claiming the attack and making demands (IBM Security, 2023).

5.2.3 Risk Factor 3: Division of Labour Tradition (Tufakanga)

This section discusses security threats caused by tufakanga, or division of labour traditions, towards CS readiness of digital HIS and data security in Tonga's hospitals. The cultural pressure of tufakanga influences the choice of study and career for many Tongans, which results in the gender gap in technical areas required for information technology and CS in hospitals and workplaces. It is previously shown (Section 4.4.3) that gender bias distorts the ratio and number of ICT and CS professionals in Tonga.

A lack of knowledge and skills in ICT becomes a threat that is caused by the lack of women seeking a career in ICT and CS. Prior discussion of the tradition of tufakanga puts men in the role of provider and protector, also claiming that computer IT exists only in the domain of men. The conservatism nature of traditional Tufakanga and gender appropriation are the reason and forces that deters Tongan women from choosing a career in computer and IT. The consequences are lack of professionals in CS and ICT as men in the field are not enough to fulfil the demand in the industry posing a risk to information and CS (Section 4.4.5). The lack of supply of IT professionals drives salaries up and makes hiring them more expensive. Hospital network organisations are usually large and demand that IT and CS professionals provide regular maintenance, therefore an absence in this area becomes a risk.

Another threat is the lack of trust whether women are ready to take on ICT and CS. Guttenbeil-Likiliki (2008) reveals an assumption in Tongan society that women cannot assume the role of leadership or perform any job equally well as men. Gender stereotyping and the lack of women in ICT present women as a vulnerable group in IT and CS. Guttenbeil-Likiliki adds that Tongan's social mentality is based on the idea that men should work and women should remain at and look after the home. While the lack of women in ICT contributes to this lack of trust, women also lack training in basic ICT knowledge, skills, and awareness and are a risk to Tonga's new digital HIS.

Discrimination against women in the corporate environment deters women from applying to ICT jobs and instead going for other roles in administration. AS3, a qualified candidate, reveals that it is difficult and almost impossible for Tongan women in ICT to climb the corporate ladder into senior roles regardless of merit and qualifications. Tongan women in ICT are treated with contempt and despised by male colleagues. Furthermore, AS3 reveals that Tongan women put down other women in ICT, a setback in efforts of women moving forward in a conservative culture. Guttenbeil-Likiliki (2008) interviews Amal Khoury and confirms the argument that Tongan women do not vote for women candidates in general elections. Also, a woman rarely sits at the head or director level in ICT or any senior position in Government ministries. Many women in Government fear other women becoming successful out of jealousy or insecurity, and society is not ready to see women assume leadership or leading roles in ICT.

The lack of women in ICT means that fewer IT professionals are available to train hospital staff regularly to better monitor the hospital's new digital HIS. The lack of IT specialists in hospitals presents a challenge in maintaining the new digital HIS and security readiness in the ICT. The toxic culture of male dominance in ICT and the equally toxic culture of women in general for not supporting other women could turn an employee into an insider threat (Luna et al., 2016).

5.2.4 Risk Factor 4: Kainga (Blood relations)

The security threats identified in Section 4.4.4 are the privilege and influence that kainga privilege possesses, which finds its way into the workplace. The privilege and influence discussed in this section are similar to the privilege created in social class discussed in Section 4.4.1. Kainga connects through family or blood relations, and the concepts of kinship and fahu privilege are the main components of kainga. Kinship describes rankings in the family, and fahu identifies who assumes that role of superiority in Tongan families. These two concepts come with privilege that is acknowledged in families or relatives (kainga) or ha'a (tribes) and often make its way into the workplace. Tonga is a tiny place, and employees with blood connections bring that acknowledgement into the workplace similar to the privilege created by

social class in Section 4.4.1. Blood relation privilege relaxes formality in the workplace, which creates casual behaviour that becomes routine over time in the organisation to the point that it becomes a culture. This casual attitude and blood privilege again create a culture of favouritism, nepotism and factions in the workplace similar to what exists in social class privilege.

The security threat identified here is produced by the blood privilege of kinship, kainga, and fahu relaxes formality in the workplace. A lack of professionalism in the workplace often leads to favouritism, nepotism and factionalism between staff seeking support and opportunity. Huang and Pearlson (2019) warns of a group's influence on shaping individual beliefs. In theory, organisations where executives and employees place high value on information security are likely to influence individual employees to follow, however this is not often the case in the Tongan context. The link between these corrupt behaviours in hospitals is staff ignoring security protocols by leaking sensitive information to third parties or using hospital networks and computers to do unauthorised activities that expose the HIS to hackers looking for a way in, or staff being the target of cybercriminals. These activities include clicking on unsafe email links or visiting unsafe websites, exposing the HIS to cybercriminals.

In the case of a security breach, compliance and obedience as cultural signs of respect are abused through blood privilege. The link between a cultural expectation of obedience and social compliance in Tongan culture is praised highly when offered for the right reason. Compliance and obedience as cultural values start at home. This value also applies in the workplace with people willingly complying out of respect until that trust is abused. There is a fine line between kind gestures and taking advantage of or abusing one's authority. A superior can request a task against work policy, and an employee respectfully obliges out of respect, fear or in return for bribery.

AS4 (Section 4.2) raises the issue of a senior staff member's refusal to learn how to use the new digital HIS and familiarise themselves with the impending changes. AS4 labels senior hospital staff as a security risk factor, even though senior members of Tongan society are highly regarded and command respect. Senior officials usually belong to the ruling class and out of respect for that, a young IT or security specialist must refrain from pressuring a superior to sit in digital technology training sessions. A young trainer would feel embarrassed to teach a senior doctor and health professional on how to use the digital systems. This relationship is similar to that of a father and son where a son out of respect cannot teach a parent and risk being scolded and frowned upon by family and elders (see Section 4.4.4). After decades of mastering a profession, it is challenging to convince senior staff to change how they do things. Senior staff may be too arrogant to learn new skills or they may prioritise time to save lives, and do not have time to spare learning CS awareness. These senior staff usually ask junior colleagues and

secretaries to help complete administrative chores while seniors focus on saving lives. The security threat is that senior employees become the weak link in the organisation's network. The vulnerable group that fails to attend CS training and is missing out on CS awareness.

5.2.5 Risk Factor 5: Gender Appropriation and Career Choice

The link between gender appropriation and risk to information security is that women do not belong in fields traditionally reserved for men, like computer IT and CS (Section 4.4.3). This attitude has long deterred many from pursuing a career in technical fields such as architecture, engineering, construction, and computers.

This research is aware of many cases of gender appropriation in the Tongan community and is confirmed by Guttenbeil-Likiliki (2008). In Table 4.2 (United Nation Women, 2022), 70% of hospital staff are women which says a lot about the social pressure on women regarding career choice and pathways. The deterrence of Tongan women from roles and careers typically filled by men is due to institutional and cultural factors (US Govt Report, 2021).

The link between gender appropriation and security threats to CS is through the human factor of power distribution between staff in hospitals. Arbel (2022) agrees there is a lack of IT professionals and this problem is a reality in Tonga, as more new qualified professionals prefer to seek employment overseas which is a security risk. To fill the need, the Government would have to hire professionals from overseas firm who charges more than permanently hiring someone local. The lack of IT and CS professionals available also means opportunities for regular training and security awareness promotions would be rare in healthcare facilities.

Healthcare staff have little IT and CS awareness but those with the appropriate level of knowledge are in the IT department. Since women users access HIS systems daily, the lack of knowledge and awareness in hospitals and Government staff is a threat to CS. Staff breach security without knowing, either by a lack of security knowledge or simply prioritising patient care over applying security measures (Swede et al., 2019). General staff assume that security is the role of IT professionals and is a role for men.

The culture and attitude is that ICT and CS matters are the job of the IT department. However, healthcare staff may not be responsible for security breaches, unauthorised sharing of sensitive information to third parties, illegal downloading, visiting unsafe websites, clicking on malicious email links and files, and exposing hospital systems to risks of cyber and ransomware attacks. Other employee-related breaches include the abuse of internal ICT or HIS systems and breaching security policies, theft of employee credentials to access the system, and stealing valuable data to sell to third parties. This behaviour exposes

hospital systems to threat actors, possibly resulting in system downtime, data breach, financial loss, harm to patients and possible loss of life (S. J. Choi & Johnson, 2019).

The lack of ICT and CS awareness in healthcare culture points back to the significance of building the right CS culture in hospitals by having the right people in executive roles (Huang & Pearlson, 2019). These are people who understand the CS role in organisations and the importance of raising a CS culture in an organisation to secure the CS of digital HIS in Tonga's hospitals.

The discrimination experienced by staff (Luna et al., 2016) may create vengeful employees who may involve themselves in incidents of cyberattack. The insider threat from human behaviour is the most challenging vector (Huang & Pearlson, 2019) emerging out of poor employment practices or an organisation with a corrupt culture.

5.2.6 Socio-Political Risk Factor 1: Foreign influence on Tonga

This section discusses security threats from foreign entities to the digital HIS in Tonga's hospitals and the findings in Section 4.4.6. This relationship between foreign states and entities threatens the CS of digital HIS in Tonga's hospitals.

Traditionally, a state's security is measured by the strength of its military and economy. Today's national security shifts to include safeguarding the digital part of the state and its functions in society. CS is a domain of modern national security where advanced digital countries use the exact requirements for developing and operating their security systems.

CS co-exists in an environment where cybercriminals target the digital capacity of states and entities. The consequence of a successful cyberattack at a state level may be extensive, where a cyberattack can cause the shutdown of state infrastructure and cause physical destruction. Typical cases of harm to critical infrastructure include power grid, transport, hospitals, nuclear plants, data warehouse, and e-Government networks.

Among the many different kinds of security threats, corruption has a significant role to play (see Section 5.2.1, Section 5.2.2 and Section 5.2.4). Cyberattacks target hardware, software, data and network systems. At the state level, the influence of powerful states and entities affects other states, especially in smaller nations like Tonga. These smaller states often become victims of bribery, conflict of interest, embezzlement, regulatory capture, state capture and procurement corruption.

An analysis of the security breach discussed in Section 4.4.6 by the GCSB and members of the Five Eyes Alliance where spying activities in the Pacific region from 2013 to 2020 are identified (Fuatai, 2024). The GCSB collects all communication through the region's satellites and marine fibre cable, including

all calls, messages and internet browsing activities from Tonga, Fiji, Samoa, Cook Islands, Tuvalu and Vanuatu. The revelation that the GCSB hosts an intelligent system that spies on neighbouring countries is a breach of trust at every level. The lack of trust affects diplomatic relations, and on a domestic level, spying activities affect everything coming and going from Tonga's internet network. Now that the e-Government is in operation, the harm is greater because all Government agencies are connecting through the Government hub.

In the case of foreign influence, manipulation of Tonga's foreign and domestic policies are a risk to Tonga's national security and the consequences of decisions impact the lives of its people (Pacific Media Centre, 2017). Tonga is fulfilling its obligation to WHO by aligning its health policy to suit WHO objectives and requirements (WHO, 2021). WHO has had controversy and corruption exposed (WHO, 2022). The security threat here is that the Tongan Government and MoH lose the power to protect its e-Government framework and digital HIS. Tonga must refrain from getting too deep into diplomacy and focus on maintaining its sovereignty and securing CS and national assets. Foreign influence impacts Tonga's domestic and foreign policies. The Government tries to please and accommodate the interests of powerful states before its own, risking state assets and weakening national security, including CS.

The Government's job at the diplomatic level is to maintain Tonga's independence to protect state assets and secure the CS of data and information in hospitals and the e-Government hub. The Tongan Government and MoH must prioritise CS in the healthcare sector to guard against international agenda and corruption Holovkin et al. (2021), leaving healthcare professionals to do its job of saving lives. MOH have no time to deal with dirty political agendas from donors and diplomatic games over control.

5.2.7 Socio-political Risk Factor 2: China as Security Threat

This section discusses how Tonga's diplomatic relations with China are a risk factor that would create security threats to CS readiness in Tongan hospitals. The findings in Section 4.4.7 reveal Tonga's ties to China is controversial.

China's unique relationship with Tonga turned the island nation into a long-term debtor to China that can now exert control over Tonga. China lent Tonga a soft loan of around USD55 million in 2007 for the rebuild of Tonga's CBD in Nuku'alofa after the 2006 riot (Figure 5.2) that destroyed 80% of the CBD (Radio NZ, 2007). The damage pressured the PM of the day, Dr Sevele, to ask China for assistance in rebuilding the infrastructure (Perry, 2019). China's officials have denied engaging in debt trap diplomacy in the Pacific during their visits to Tonga in June 2022 (Figure 5.3). The visit includes a discussion of the loan on the agenda for the meeting, however what China may want in return is questioned. Land,

Figure 5.2: Tonga's CBD burned down by pro-democratic rioters on November 16,2006 (Radio NZ, 2019)

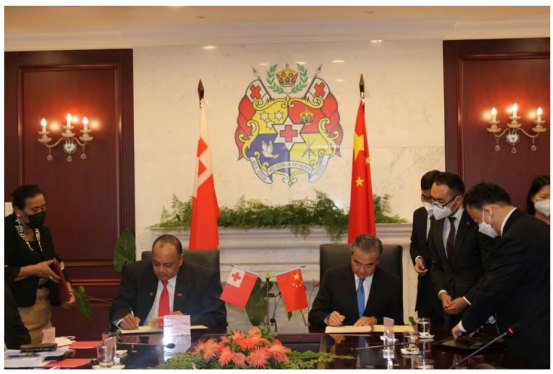

Figure 5.3: Tonga's Government host China's diplomats in Nuku'alofa.June 2022 (The Guardian, 2022)

information, a window to Australia and New Zealand, or influence in the Pacific are all possibilities. A media interview with Mr Teisina Fuko, a Tonga political figure, says that Tonga is vital for China's influence in the South Pacific and also a stepping stone or a window to New Zealand and Australia since the trio are very close (Perry, 2019). Fuko reveals that it is much easier for China to get through Tonga.

Tonga's current situation as a debtor to China puts Tonga in a precarious position. Tonga could lose its independence as a nation, its liberty to make decisions, the power to negotiate, to challenge and criticise, and to stand firm as a sovereign nation. China is so powerful that it could implement economic sanctions on trade as it already imposed on Canada for three years (CBC, 2022).

China now has the advantage of asking for anything from the Tongan Government. Fishing rights, business deals, harvesting marine resources off Tongan waters, or using Tonga for whatever project China has in mind. China could take Tongan land as a form of payment on a 99-year lease, similar to how a Chinese company has taken over Sri Lanka's Hambantota Port for failing to pay $1.12 billion on a 99-year lease (Nikkei Asia, 2024). China could ask for access to systems or information it wants from

Tonga, or it could just go ahead and get it as China has the resources and capability to hack into any system as revealed by the Office of the United States Trade Representative (2018).

Tonga is at risk of being a target of cyber intrusion from China because of Tonga's position in the Pacific, diplomatic ties with Western Allies, and the influence these countries have in the Pacific. Alongside Fiji and many other Pacific nations, Tonga are members of the Commonwealth, which ties these nations to Britain and other Western Allies. The investigation report in (Office of the United States Trade Representative, 2018) reveals China utilises cyber intrusion techniques to gain access to valuable information on sensitive and proprietary internal communication, negotiation positions, trade secrets, and technical data that serve any of its strategic objectives, either economic, political, or military.

China's increased activities in the Pacific prompted the US, Britain, Australia, and New Zealand to respond with tours around the Pacific nations to secure its place and influence. The US confirmed its presence by opening its first Embassy in Tonga's capital, and Britain followed by reopening the High Commissioner Office after its closure in 2006. Tonga is talking to both sides, which puts Tonga in a dangerous position of becoming a security target. Maybe Tonga's new e-government network is already on zero-day attack, and no one has noticed. China would like to know what is on the agenda of every meeting and every interaction between Tonga and members of the Western Allies.

Another security threat focuses on Chinese-made computer smart devices. The US Government investigation on China's illegal cyber hacking into US businesses Office of the United States Trade Representative (2018) raises serious security concerns that result in sanctions against China's tech giant Huawei. The sanction orders the ban of all Chinese-made computer and CCTV equipment from Government facilities across the United States, Britain, and Australia (Australian Institute of Internal Affairs, 2023). The US sanction of Huawei in 2018 is a response to security concerns and credible evidence of Chinese technology failing to comply with US laws and strong ties to the Chinese Government. The ban on Huawei smartphone products and wireless technology are effective in the US, Australia, Japan, Taiwan, and New Zealand. More European countries later joined, including Denmark, France, Germany, Italy, Portugal, Latvia, Lithuania, Romania, Sweden, and Estonia (Reuters, 2023). These countries have phased out Huawei products from their network. The UK banned Huawei from contributing core parts to 5G technology, cutting the Chinese giant's share in the country's network to 35%. The US, Australia, and Britain in 2018 banned Chinese-made CCTV equipment from politicians' properties and government buildings. Aljazeera (2018) reports that China supplies Iran and North Korea with Huawei technology, which allows its Government to spy on people.

Tonga is well aware of the illegal activities that China is involved in, but Tonga is in no position to

challenge nor refuse any offer from China. China's gift of the St.George Palace and Tonga High School complex are equipped with computer equipment and internet network donated by China (Aid Data, 2017; Fonua, 2003). This raises a security concern as St.George houses the PMO, Foreign Affairs, and Treasury (until 2023). China may not donate or supply computer equipment to hospitals (Asian Development Bank, 2019). However, hospital networks connect to the e-Government hub and data warehouse, which operates on China's Huawei technologies. The Government's proposal to connect G-Cloud to a Huawei data centre compromises the security, storage, and management of data independently.

The Tongan e-Government and its network, including the MoH, are at risk of malware attacks via spyware, ransomware, viruses, bots, keyloggers, worms, and crypto-jacking. A successful cyberattack could harm hospitals and their networks, resulting in loss of data and service availability. In Section 2.3.2, G. Martin et al. (2017) explain that once medical data is accessed and touched by cybercriminals, it loses its integrity and is unusable. It is wise for hospitals to save multiple copies in different locations to save the hospital from unrecoverable loss of information and expensive damage in the near future.

5.3 Recommendations and Contributions

This section provides a summary of recommendations.

Governance Hospitals must have the right governance processes to ensure organisational health and security. These include sound CS policies and legislation that are up to date and are enforceable through internal disciplinary procedures and by law.

1. Executives must have sound and updated knowledge of CS and awareness. Also an understanding of how to apply this knowledge in hospital infrastructure.
2. Executives and leaders create CS culture in hospitals by being good role models. Leaders must be reminded of this responsibility from time to time.
3. Executives as creators of CS culture must have proper training and support in place in order to execute this job effectively (Bhuyan et al., 2020).
4. Alshaikh (2020) recommend establishing a CS champion network in hospitals. This network helps the CS team amplify CS awareness throughout the organisation and the ears and eyes for the ICT on the ground.

Legislation In relation to CS...

1. Tonga must have legislation in place specific to CS and information security to protect its new e-Government infrastructure and the digital HIS in hospitals. The US HIPAA is an excellent example of an effective legislation mandate across the US enforceable by law enforcement (Langer, 2016).
2. International and local government role in combating cybercrime and the need for coordinated action between state governments and the international community to harmonise domestic cybercrime laws and international efforts to combat cybercrimes (Clough, 2014).
3. Future law must provide tough punishment for culprits of security in hospitals. Touch laws would discourage individuals from being bad actors and corruption in agencies.
4. Hospitals and health facilities must have an Emergency Readiness Plan in place that utilises all-hazard approaches, including CS. Future legislation must make this compulsory.
5. Future law must mandate the installation of electronic security systems and efficient antiviral computer software in hospitals in order to identify, stop, and guard against viruses and malware which are frequently employed in cyberattacks and that could damage or even wipe out their information systems (Centers for Medicare and Medicaid Services, 2016).

Strict CS Policy Policy ought to include...

1. Advocating for strict security policy in hospitals must be enforced with disciplinary actions for those who fail to comply (Bhuyan et al., 2020).
2. All employees' identities as digital HIS users must be verified by privileged access management in place.
3. Security capabilities must be in place to verify and protect all user and infrastructure devices in hospitals and health facilities from access by bad actors. Infrastructure devices include security cameras, smart printers, and medical devices connected to the hospital network.
4. Implement security controls for user access where all employees are only given access privileges according to each job requirement and nothing more.
5. Security capability that tracks all user's access to a patient's files and flags unauthorised access unless the user is a direct carer of that particular patient must be in place.
6. Network segmentation policy based on identity ranking and different departments of the MoH must be in place.

Training and communication Recommendations provide that ...

1. Designing training programs must be fun and easy for non-technical people to understand. For example, the use of visual training that is informative, fun and educational to test and update users' knowledge. Benjamin. D. Cone and Nguyen (2007) illustrate the success of video games in CS training.
2. Fill the knowledge and skills gap in ICT by encouraging more women to study and build a career in the field to help relieve the lack of computer and CS professionals available in Tonga.
3. Cultural Sensitivity in CS Training. Management and employees alike should be aware of the importance of maintaining a strict policy that upholds respect for CS as well as respecting the local social culture that would also combat cultural risk factors discussed earlier in this thesis.

Technology tools CS protection and detection tools ought to include...

1. Enhanced technical solutions such as Threat Intelligence capabilities to detect real-time threats and use of Artificial Intelligence (AI).
2. Zero-trust modelling where a security framework that screens all users within the hospital's network through authentication, authorisation, and constant validation for security configuration and posture before access is granted for application and data. The hospital network includes local, G-Cloud, and hybrid with resources and users across the network.
3. Maintain data sovereignty so that hospital policy and protocols on data handling and security must abide by the law of Tonga. That data privacy and security must be protected and respected by both local and international entities.
4. Regular audits and compliance checks are put in place to ensure that security policies and conducts in Tonga's hospitals adhere to codes of conduct, rules, regulations and international standards. These audits are required to review the effectiveness of an organisation's internal control.
5. IT security team patches commonly used software vulnerabilities.
6. Patch commonly exploited by cybercriminals are Microsoft products such as Internet Explorer, Office Word, Excel and PowerPoint; Oracle products; and some Adobe products such as Reader Acrobat and OpenSSL.

7. The Government takes a centralised approach to the new digital HIS. Therefore, deploying firewalls with built-in intrusion prevention systems and network behaviour anomaly detection tools is essential. Packet Capture and Sensor Tools must be added to hospital security (Ghosh, 2023).
8. Shifting HIS operations or parts into the G-Cloud is more secure, cheaper and effective for managing and deploying applications. Serverless architecture guarantees protection for application workloads in Tonga's present digital landscape.
9. MoH must protect data from unauthorised access, use, disclosure, modification, disruption and destruction. Security tools mentioned earlier are crucial, but data backup in remote locations is compulsory.
10. Up-to-date Incident Response and Disaster Recovery Plans that detail how Tonga's hospitals can recover data, restore operations and continuous functions of hospitals after a disastrous event such as a data breach from a natural disaster, cyber-attack or human error.

Continuous campaign Continue to raise awareness in areas of...

1. Campaign must raise over gender-based discrimination in ICT at the corporate level and in the workplace. The campaign would educate people and change the attitude and stereotyping of women in male-dominated fields.
2. Increase public understanding and awareness of the significance of CS and information security in maintaining service and delivery in hospitals as critical facilities.
3. Raise awareness of the importance of CS awareness and safety practice as a user of systems in healthcare facilities. Safety practices minimise any chances of security breaches and allow cybercriminals to get into the system.
4. Raise awareness of the cultural risk factors raised in this research and the threats to CS readiness of hospitals and health facilities in Tonga.
5. The campaign must remind employees that CS is everybody's business and that everyone as a user is equally responsible for the security of systems and data in hospitals.
6. Teaching CS awareness must spread into the communities, and CS information must be accessible to the public to build a healthy CS culture in Tongan society.
7. The most effective campaign mode in Tonga is through television, radio broadcasting networks, social media, fono or community meetings.

5.4 Conclusion

This chapter addresses the research question and the analysis of findings in Chapter 4. The results identify five cultural and two socio-political risks. Cultural risk factors found are pervasive, raising a high level of concern over the CS readiness of the digital HIS in Tongan hospitals, involving executives, staff, and a lack of attention to cultural risks in the workplace. Tonga's e-Government framework and the hospital's digital HIS are still in the early years of trial and error, and staff are getting used to the new system. It is necessary to spread the word about the importance of being CS secure and risk awareness (Arbel, 2022). Advanced technology alone cannot secure hospital systems and data security if there are vulnerabilities among the users exposed to the cultural risks identified by this research.

The chapter recommends advice to mitigate risk. This research finds that social and cultural risks are best managed by education, training, strict security policy, and sound legislation (Bhuyan et al., 2020). This research also finds that organisational culture can develop into a better, healthier, and more effective culture for hospitals led by executives and leaders. The cultural risk case of Tonga is complex and challenging. However, there is always hope that this research will help find a way to mitigate the cultural issues to secure an effective security culture for hospitals and a great role model for other agencies in Tonga.

The next chapter provides the conclusion to this thesis and summarises the research, its findings, and conclusions. The following chapter also identifies further research opportunities.

Chapter 6

Conclusion

6.1 Introduction

In the previous chapter, the results of the analysis are discussed and recommendations are made to guide the development of CS in the deployment of the Tongan digital HIS. To conclude the thesis, this chapter summarises the research, focusing on the significance of social and organisational culture and its impact on CS in Tongan hospitals. This study argues that building a positive and safe culture from the top down in hospitals and the health sector is possible. The research results create grounds for recommendations and further study.

6.2 Summary of Research

This research investigates Tongan culture to identify the risks it could pose against information security and privacy, focusing on Tongan hospitals. The research targets cultural traditions, practices, and ideologies that influence how Tongans behave socially and in the workplace.

Chapter 1 introduces the research topic of the cultural risk factors that identify CS to digital HIS at hospitals in Tonga. This chapter also outlines the thesis structure and covers the background and motivation for the research. The literature review in Chapter 2 presents the security challenges hospitals face in the healthcare industry worldwide due to increasing cyberattacks. The review also reveals why hospitals are important as critical infrastructure and why they deserve strict protection. The second part of the literature review demonstrates valid concern over the significant role of organisational culture in the success and failure of CS. The literature reviewed on CS culture in organisations is Western-oriented,

and no study is available on ethnic culture in either CS or organisational context.

Comparative studies on the significance of having the right culture in the workplace and how to build a sound security culture in hospitals present themselves in Chapter 2. A review of why healthcare is a popular target for cyberattacks and the motives and consequences of weak security is also covered. Hackers are targeting hospital systems to steal data to sell in the black market, and literature reveals that hospital systems are hackable due to a lack of funding and resources to secure the HIS in hospitals.

The review discovers the gap that leads to formulating the research question this research addresses.

Research Question

What are the cultural risk factors in the Tongan cultural context that identify as security threats to the CS readiness of digital HIS in Tonga?

An appropriate methodology for conducting the research is provided in Chapter 3. The chapter describes the collection and analysis of data to address the research question. Interpretive research design was chosen as the approach due to the sensitive nature of the study issue for a number of reasons. This design involves observation and documentaries remotely away from the setting. The option of interview and survey is excluded because key people refuse to get in touch due to employment and legal obligations and the worries of being socially scrutinised for their opinions or sharing information. However, other people offer information in return for anonymity. The sources utilised are culture, people, experiences, video footage, and literature.

The application of the method produces data that are analysed in Chapter 4. These findings identify five cultural and two socio-political risk factors and demonstrate how these cultural traditions are considered a security threat to hospital CS readiness. The results of this study raise serious concerns over the security and readiness of hospitals in Tonga.

The findings in Chapter 4 identify seven risk factors, two of which are socio-political factors. Risk factors 1 through 2 are socio-structural related to social class and the centralisation structure in the new eGovernment and the risks from a cultural context. Cultural Risk 1 and 2 reflect the Tongan social and political structure in the form of inequality both outside and inside the workplace, then in a negative tone that affects employment culture and the morale of people as users of systems. When culture is toxic, and morale is low, there is a high risk of corruption and human error that leads to security breach, which are threats to CS. Risk factors 3 to 5 are socio-gender related, with division of labour, gender appropriation, kinship and blood relations as risk factors due to discrimination, nepotism, favouritism, and factions commonly seen in hospitals and other organisations across the board. Gender appropriation and division of labour are to blame for the lack of women in ICT and the lack of IT and CS professionals in Tonga,

which create a risk to the newly rolled out eGovernment and digital HIS in hospitals. The casual attitudes and toxic culture in many workplaces are linked to a culture where women are perceived as inferior in the workplace due to gender rather than merit.

Risks 6 and 7 are sociopolitical, with a focus on foreign influence and a particular case on China's influence. Diplomatic pressure influences both domestic and foreign policies in Tonga to suit the agendas of donors and requirements of foreign entities that do not have the interest of Tonga as a priority. The case of the Five Eyes spies in the Pacific is an example of diplomatic influences and connections. Risk 7 is the case of China as a security threat to Tonga and the HIS in hospitals. The reputation of China as a bad actor in CS internationally is big enough to be a CS risk on its own. Tonga must protect its independence and assets from succumbing to external demand in return for aid and support.

Chapter 5 examines and discusses the findings and the links to security threats and linking each back to the literature review in Chapter 2, and more crucially, addresses the research question this research proposes. Moreover, some suggestions aim to improve data security and privacy, manage cultural issues at work, and establish a safe environment for employees using digital HIS. The research also offers recommendations based on the cultural risk factors uncovered during this research including governance, legislation, policy, technology and post-campaign activities.

6.3 Research Methods and Limitations

The methodology design for this research utilises observation and documentation methods to access, gather data and analyse results. This entire study is conducted remotely outside Tonga, which is challenging but achievable. Access to information and people relevant to the research matter is difficult, but other resources are used to mitigate that.

The exclusion of interviews and surveys is predetermined because people may only participate if it is anonymous. The reasons are employment and legal obligations and fear of social scrutiny. However, a limited number of pertinent subjects willing to speak in exchange for anonymity; this is also noted in Section 4.2

There is no similar research on cultural and socio-political risk in Tonga, therefore this research may be the first of its kind to fill the gap. Finding relevant peer-reviewed literature on cultural factors related to CS and information security is challenging, but the research is managed with what is available.

6.4 Future Research

Several potential additional research areas are available to improve the overall knowledge and understanding of socio-political and cultural phenomena in Tonga and how these create security risks. This study identifies Tongan society's cultural and socio-political vulnerabilities that could compromise information security and privacy. Further research focuses on the cultural factor of violence and sexual abuse in Tongan society and the possible link to information security risks. Data exists and is as high as 1 in every 3 women are affected by violence and sexual abuse. There is a lack of information on the damage to mental and physical health and the impact on the workplace and CS. Further research into the gender gap in computers and IT will be conducted to solve this problem by identifying the challenges and what is needed to mitigate them.

Another area of research is the need to find a solution or how to mitigate social problems uncovered in this research. The cultural risks in this research identify the need for good legislation as the backbone of a great CS structure in Tonga. There is a need for sound legislation that would satisfy the legal requirements for a healthy CS in Tonga by identifying the gaps and what needs to be done. Take the US HIPAA law as an example. The legislature must be monitored and enforceable by the Court of Justice and the police.

To identify gaps and draft a sound security policy, further research is required in a review of the current security policy and regulation in the MoH. The ministry must enforce this policy via disciplinary action and further referral to an independent body, such as the Ombudsman in Tonga if the problem is not resolved. A good security policy could set new standards within the healthcare sector and be transferable to other agencies and organisations.

Research into the CS readiness of hospitals in Tonga by conducting quantitative methods is required. Methods to determine the level of knowledge, understanding and awareness among hospital employees. Establish the state of CS culture in the workplace. Current staff attitudes towards CS and data security. This survey could identify the gaps and formulate a plan to mitigate issues raised from the survey, such as proposed training, policy and legislation updates and campaigns.

6.5 Conclusion

HIS and networks have increasingly moved to digital and innovative technology to deliver services and increase productivity and convenience, but are exposing data security to internal errors and cyberattacks. This research identified and reported potential vulnerabilities in Tongan culture that threaten data security and information privacy in hospitals' digital HIS.

This study identifies that women represent the majority of hospital HIS system users, posing a more significant risk than men due to a lack of IT and CS knowledge and skills. This research is essential to uncover the cultural risks in Tongan society and the potential harm it could cause to hospitals' HIS. It focuses on female users as a high-risk group that requires immediate education and training.

Mitigating future risks to hospital HIS and data and information security may require joint efforts of hospital leadership and its IT department by prioritising and designing practical training and reviewing security policies, monitoring both HIS and users, and legislation to protect data security and information privacy. CS awareness must begin its cultivation in hospitals from the top to build the right CS culture in the workplace.

References

Ahmed, M. & Litchfield, A. T. (2016). Taxonomy for identification of security issues in cloud computing environments. *Journal of Computer Information Systems*, *58*(1), 79–88. doi: https://doi.org/10.1080/08874417.2016.1192520

Aid Data. (2017). *Chinese government donates furniture and equipment worth usd590,000 to tonga high school* [Web Page]. Retrieved 2023-03-21, from `https://china.aiddata.org/projects/39228/`

Alhogail, A. & Abdulrahman, M. (2014, 1 September). A proposal of an organizational information security culture framework. In *Proceedings of international conference on information, communication technology and system (icts) 2014* (p. 243-250). Saudi Arabia. doi: https://doi.org/10.1109/ICTS.2014.7010591

Aljazeera. (2018). *Why are countries banning huawei?* [Web Page]. Retrieved 2023-11-16, from `https://shorter.me/Urue3`

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers and Security*, *98*(1), 1-4. doi: https://doi.org/10.1016/j.cose.2020.102003

Arbel, N. (2022). *The widening cybersecurity talent gap and its ramifications in 2022* [Web Page]. Retrieved 2023-03-28, from `https://shorter.me/dmLjW`

Asian Development Bank. (2019). *Tonga: Introducing egovernment through digital* [Web Page]. Retrieved 2023-07-09, from `https://www.adb.org/projects/50281-001/main`

Astakhova, L. (2014). The concept of the information security culture. *Scientific and Technical Information Processing*, *41*(1), 22–28. doi: https://doi.org/10.3103/S0147688214010067

Australian Institute of Internal Affairs. (2023). *Regulating chinese-made cctv cameras in australia* [Web Page]. Retrieved 2023-04-02, from `https://shorter.me/_Alii`

Bada, M., Von Solms, B. & Agrafiotis, I. (2019). Reviewing national cybersecurity awareness in africa: An empirical study. *International Journal on Advances in Security*, *12*(1), 9–25. Retrieved from `https://arxiv.org/pdf/1910.01005` doi: 10.48550/arXiv.1910.01005

Bassett, G., Hylender, D. C., Langlois, P., Pinto, A. & Widup, S. (2021). *DBIR: 2021 Data Breach Investigations Report.* [Web Page]. Retrieved 2023-02-16, from `https://shorter.me/dfGR7`

Benjamin. D. Cone, M. F. T., Cynthia Irvine & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computer and Security*, *26*(1), 63–72. doi: http://dx.doi.org/10.1016/j.cose.2006.10.005

Bergal, J. (2022). *Ransomeware attacks on hospitals put patients at risk* [Web Page]. Retrieved 2023-04-16, from `https://shorter.me/1YtWD`

Bhattacherjee, A. (2012). *Social science research-principles, methods, and practices* (3rd ed.). Florida, USA: Global Text Project.

Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., ... Dasgupta, D. (2020). Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. *Journal of medical systems*, *44*(98), 1–9. doi: https://doi.org/10.1007/s10916-019-1507-y

Blythe, J. M., Gray, A. & Collins, E. (2020, 19–24 July). Human cyber risk management by security awareness professionals: Carrots or sticks to drive behaviour change? In *Hci for cybersecurity,*

privacy and trust: Second international conference, hci-cpt 2020 (pp. 76–91). Copenhagen, Denmark. doi: https://doi.org/10.1007/978-3-030-50309-3_6

Bott, E. (1981). Power and rank in the kingdom of tonga. *The Journal of the Polynesian Society*, *90*(1), 7–81. Retrieved from https://www.jstor.org/stable/20705538

Britannica. (2024). *Cultural appropriation* [Web Page]. Retrieved 2024-04-17, from https://shorturl.at/hoKT8

Campean, S. (2019). The human factor at the center of a cyber security culture. *International Journal of Information Security and Cybercrime (IJISC)*, *8*(1), 51–58. doi: http://dx.doi.org/10.19107/IJISC.2019.01.07

Campos, P. A. & Reich, M. (2019). Political analysis for health policy implementation. *Health Systems and Reform*, *5*(3), 224–235. doi: https://doi.org/10.1080/23288604.2019.1625251

Carrillo, R. A. (2010). Positive safety culture: How to create, lead and maintain. *Professional Safety*, *55*(5), 47–54. Retrieved from https://shorter.me/QcmWk

CBC. (2022). *China has lifted a 3-year ban on canadian canola, ottawa says* [Web Page]. Retrieved 2023-05-06, from https://shorter.me/9PHxI

Centers for Medicare and Medicaid Services. (2016). *Homeland security threats* [Web Page]. Retrieved 2023-06-03, from https://shorter.me/wuTPW

Choi, M. (2016). Leadership of information security manager on the effectiveness of information systems security for secure sustainable computing. *Sustainability*, *8*(7), 638. doi: https://doi.org/10.3390/su8070638

Choi, S. J. & Johnson, M. E. (2019). *Do hospital data breaches reduce patient care quality?* [Web Page]. doi: https://doi.org/10.48550/arXiv.1904.02058

Choudhry, R. M., Fang, D. & Mohamed, S. (2007). The nature of safety culture: A survey of the state-of-the-art. *Safety science*, *45*(10), 993–1012. doi: https://doi.org/10.1016/j.ssci.2006.09.003

Clarke, R. & Youngstein, T. (2017). Cyberattack on brittain's national health services–a wake up call for modern medicine. *The New England Journal of Medicine.*, *377*(1), 409–411. doi: 10.1056/NEJMp1706754

Clough, J. (2014). *A world of difference: The budapest convention on cybercrime and the challenges of harmonisation* [Web Page]. Retrieved 2023-08-21, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2615789

Coiera, E., Aarts, J. & Kulikowski, C. (2011). The dangerous decade. *Journal of the American Medical Informatics Association*, *19*(1), 2–5. doi: https://doi.org/10.1136/amiajnl-2011-000674

Commonwealth of Learning. (2014). *Gender profile:tonga* [Web Page]. Retrieved 2023-06-18, from https://shorter.me/yPn4P

Coventry, L. & Branley, D. (2018). Cybersecurity in healthcare:a narrative review of trends, threats and ways forward. *Maturitas*, *113*(1), 48–52. doi: https://doi.org/10.1016/j.maturitas.2018.04.008

Cremer, J. (1993). Corporate culture and shared knowledge. *Industrial and corporate change*, *2*(3), 351–386. doi: https://doi.org/10.1093/icc/2.3.351

Cybersecurity and Infrastructure Security Agency. (2021). *Security tip (st04–015): Understanding denial-of-service attacks.* [Web Page]. Retrieved 2023-07-12, from https://shorter.me/zIQCf

Cybersecurity and Infrastructure Security Agency. (2023). *What is network segmentation* [Web Page]. Retrieved 2023-07-12, from https://shorter.me/jYouL

Da Veiga, A. (2016). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. In *Proceedings of 2016 sai computing conference* (pp. 1006–1015). London, UK. doi: http://dx.doi.org/10.1109/SAI.2016.7556102

Da Veiga, A., Astakhova, L. V., Botha, A. & Herselman, M. (2020). Defining organisational information security culture- perspectives from academia and industry. *Computers and Security*, *92*(1), 101713. doi: https://doi.org/10.1016/j.cose.2020.101713

Da Veiga, A. & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers and security*, *29*(2), 196–207. doi: https://doi.org/10.1016/j.cose.2009.09.002

Da Veiga, A. & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers and Security*, *70*(1), 72–94. doi: https://doi.org/10.1016/j.cose.2017.05.002

Department of the Prime Minister and Cabinet. (2019). *New zealand cyber security strategy 20192003* [Web Page]. Retrieved 2024-08-30, from https://shorturl.at/2xkaZ

Dhillon, G. (1997). Principles for managing information system security. In *In:managing information system security. information systems series* (pp. 137–172). Palgrave, London: Print ISBN. doi: https://doi.org/10.1007/978-1-349-14454-9_6

Dobberstein, L. (2023). *Australian gives made-in-china cctv cams the boot* [Web Page]. Retrieved 2023-05-16, from https://shorter.me/x8prx

Dullea, E., Budke, C. & Enko, P. (2020). Cybersecurity update: Recent ransomware attacks against healthcare providers. *Mo Med*, *117*(6), 533–534. Retrieved from https://shorturl.at/nrHIU

ENLITIC. (2023). *Deidentifying and anonymising healthcare data* [Web Page]. Retrieved 2024-09-19, from https://shorturl.at/ZrOz1

Federal Bureau of Investigation. (2022). *Internet crime report 2022* [Web Page]. Retrieved 2023-02-17, from https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Field, M. (2014). *Tonga democracy mp becomes prime minister* [Web Page]. Retrieved 2023-04-05, from https://shorter.me/yArNA

Filihia, M. (2001). Men are from maama, women are from puluto: Female status in tongan society. *The Journal of the Polynesian Society*, *110*(4), 337–390. Retrieved from https://www.jstor.org/stable/20707020

Fonua, P. (1998). *China switch brings tonga closer to un dream* [Web Page]. Retrieved 2023-01-16, from https://shorter.me/VA6Uu

Fonua, P. (2003). *Tonga high rises from the ashes* [Web Page]. Retrieved 2023-04-20, from https://matangitonga.to/2003/12/30/tonga-high-rises-ashes

Forbes. (2020). *Ccpa fines, fraud and fragmented data* [Web Page]. Retrieved 2023-06-13, from https://shorter.me/3oKeg

Fuatai, T. (2024). *Spying on our pacific family.* [Web Page]. Retrieved 2024-03-31, from https://shorter.me/sWvnY

Garfinkel, S. L. (2015). *De-identification of personal information* [Web Page]. Retrieved 2024-09-19, from https://nvlpubs.nist.gov/nistpubs/ir/2015/nist.ir.8053.pdf

Gcaza, N., Van Vuuren, J. J. & Von Solms, R. (2015, June). An ontology for a national cybersecurity culture environment. In *Ninth international symposium on human aspects of information security & assurance (haisa 2015)* (pp. 1–9). Retrieved from https://shorter.me/Jzntw

Geertz, C. (1985). Local knowledge: Further essays in interpretive anthropology. *Annals of the Association of American Geographers*, *75*(2), 291–293. Retrieved from https://www.jstor.org/stable/2562574

Ghosh, S. C. (2023). *The five pillars of cisco's cyber readiness index* [Web Page]. Retrieved 2024-02-16, from https://ciosea.economictimes.indiatimes.com/news/security/the-five-pillars-of-ciscos-cyber-readiness-index/99240944

Giansanti, D. & Monoscalco, L. (2021). The cyber-risk in cardiology: towards an investigation on the self-perception among the cardiologists. mhealth. 2021. *mHealth*, *7*(1). doi: https://doi.org/10.21037/mhealth.2020.01.08

Government of Tonga. (2016). *Constitution of tonga* [Web Page]. Retrieved 2023-07-12, from https://faolex.fao.org/docs/pdf/ton132921.pdf

Government of Tonga. (2019). *Computer crimes bills 2019* [Web Page]. Retrieved 2024-08-30, from https://shorturl.at/FeXiv

Greig, A., Renaud, K. V. & Flowerday, S. (2015). An ethnographic study to assess the enactment of information security culture in a retail store. In *2015 world congress on internet security (worldcis)* (p. 61-66). Dublin, Ireland: IEEE. doi: https://doi.org/10.1109/WorldCIS.2015.7359415

Grimes, S. & Wirth, A. (2017). *Holding the line: events that shaped healthcare cybersecurity–biomed instrument technol.* [Web Page]. doi: doi:10.2345/0899-8205-51.s6.30

Guttenbeil-Likiliki, O. (2008). *Report4: Women's representation in tonga* [Web Page]. Retrieved 2023-02-16, from https://shorter.me/xBzs0 (Last accessed 16 February 2023)

He, Y., Aliyu, A., Evans, M. & Luo, C. (2021). Health care cybersecurity challenges and solutions under the climate of covid-19: Scoping review. *Journal of Medical Internet Research*, *23*(4), 1. doi: https://doi.org/10.2196/21747

Health Policy Watch. (2023). *How does corruption affect healthcare worldwide?* [Web Page]. Retrieved 2024-03-07, from https://shorter.me/4exF2

Healthcare Information and Management Systems Society. (2022). *2020 himss cybersecurity survey* [Web Page]. Retrieved 2023-02-16, from https://www.himss.org/resources/himss-healthcare-cybersecurity-survey

Helu, F. (1995). Brother/sister and gender relations in ancient and modern tonga. *Journal de la Societe des Oceanistes*, *100*(1), 191–200. Retrieved from https://www.persee.fr/doc/jso_0300-953x_1995_num_100_1_1963

Hernandez, J. (2024). *Dark web statistics & trends for 2024* [Web Page]. Retrieved 2024-04-06, from https://ln.run/7YCv_

Hill, B. (2016). *Tongan reporter suspended on pm pohiva's orders.* [Web Page]. Retrieved 2023-04-14, from https://shorter.me/wpZDO

Holovkin, B. M., Tavolzhanskyi, O. V. & Lysodyed, O. V. (2021). Corruption as a cybersecurity threat in the new world order. *Connections: The Quarterly Journal*, *20*(2), 75–87. Retrieved from https://doi.org/10.11610/Connections.20.2.07

Huang, K. & Pearlson, K. (2019, 8 January). For what technology can't fix: Building a model of organisational cybersecurity culture. In *Proceedings of the 52nd hawaii international conference on system sciences* (pp. 6398–6407). Honolulu, Hawaii. doi: https://doi.org/10.24251/HICSS.2019.769

Huang, K., Siegel, M. & Madnick, S. (2018). Systematically understanding the cyber attack business: A survey. *ACM Computer Survey*, *51*(4), 1–36. doi: https://doi.org/10.1145/3199674

IBM Security. (2020). *A million-dollar race to detect and respond* [Web Page]. Retrieved 2023-05-01, from https://www.ibm.com/downloads/cas/3R8N1DZJ

IBM Security. (2023). *Cost of a data breach report 2023* [Web Page]. Retrieved 2023-05-16, from https://www.ibm.com/reports/data-breach

Ioannou, M., Stavrou, E. & Bada, M. (2019). Cybersecurity culture in computer security incident response teams: Investigating difficulties in communication and coordination. In *2019 international conference on cyber security and protection of digital services (cyber security)* (pp. 1–4). Oxford, UK. doi: https://doi.org/10.1109/CyberSecPODS.2019.8885240

ISO. (2013a). *Iso/iec 27000:2018 information technology: Security techniques information security management systems overview and vocabulary* [Web Page]. Retrieved 2023-05-08, from https://www.iso.org/standard/73906.html

ISO. (2013b). *Iso/iec 27000:2018 information technology: Security techniques information security management systems overview and vocabulary* [Web Page]. Retrieved 2023-05-08, from https://www.iso.org/standard/73906.html

James, K. (1990). Gender relations in tonga:paradigm shift. *Tongan Culture and history*, *1*(1), 217–230. Retrieved from https://ehrafworldcultures.yale.edu/document?id=ou09-132

James, K. (1992). Tongan rank revisited: Religious hierarchy, social stratification, and gender in the ancient tongan polity. *Social Analysis: The International Journal of Anthropology*, *1*(31), 79–102. Retrieved from https://www.jstor.org/stable/23164561

James, W. (2022). *Uk restrict chinese cameras in government buildings over security fears* [Web Page]. Retrieved 2023-02-16, from https://shorter.me/CrSIx

Japan International Cooperation Agency. (2010). *Country gender profile: The kingdom of tonga* [Web Page]. Retrieved 2023-06-27, from https://shorter.me/2sRSg

Jordan, J. (2023). *Exploring the link between corruption and cybercrime* [Web Page]. Retrieved 2024-03-08, from https://shorter.me/NzaG_

Justice, M. o. (2003). *Privacy law act 2003* [Web Page]. Retrieved 2024-08-30, from https://shorturl.at/HKmcH

Justice, M. o. (2020). *Privacy law act 2020* [Web Page]. Retrieved 2024-08-30, from https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html

Kaeppler, A. L. (1971). Rank in tonga.ethnology. *An International Journal of Cultural and Social Anthropology*, *10*(2), 174–193. doi: https://doi.org/10.2307/3773008

Kelpsas, B. & Nelson, A. (2016, September). Ransomware in hospitals: what providers will inevitably face when attacked. *The Journal of Medical Practice Management*, *32*(1), 67–70. Retrieved from https://pubmed.ncbi.nlm.nih.gov/30452851/

Kuhn, T. & Musgrave, A. (1970). Proceedings of the international in the philosophy of science. In *Criticism and the growth of knowledge* (p. 282). London, United Kingdom: Cambridge University Press. Retrieved from https://l1nq.com/8dvTn

Langer, S. G. (2016). Cyber-security issues in healthcare information technology. j dig imag. *Journal of Digital Imaging*, *30*(1), 117–125. doi: https://doi.org/10.1007/s10278-016-9913-x

Laulaupeaalu, S. (2016). *Cyber security vulnerabilities in tonga* (Unpublished doctoral dissertation). Waikato University.

Lee, J., McCullough, J. S. & Town, R. J. (2012, April). The impact of health technology on hospital productivity. *NBER Working Paper No,18025*, *18025*(1). doi: https://doi.org/10.3386/w18025

Leidner, D. E. & Kayworth, T. (2006, June). Review: A review of culture in information systems research: Towards a theory of information technology culture conflict. *MIS Quarterly Review*, *30*(2). doi: https://doi.org/10.2307/25148735

Luna, R., Rhine, E., Myhra, M., Sullivan, R. & Kruse, C. S. (2016). Cyber threats to health information systems: a systematic review. technol health care. *Technology and Health Care*, *24*(1). doi: https://doi.org/10.3233/THC-151102

Lutui, P. R. (2021). *Critically examine the readiness of tonga's legislative framework for e-crimes* (Unpublished doctoral dissertation). Auckland University of Technology.

Ma'a Fafine Tonga Inc. (2010). *National study on domestic violence against women in tonga* (1st ed.). Nuku'alofa, Tonga: Ma'a Fafine mo e Famili 2012.

Manch, T. (2021). *Trade minister damien o'connor warns parliamentary debate on xinjiang genocide would damage trade* [Web Page]. Retrieved 2024-01-08, from https://shorter.me/-Knb2

Marotta, A. & Pearlson, K. (2019, 1 March). A culture of cybersecurity at banca popolare di sondrio. In *Amcis 2019 proceedings* (pp. 1–10). Massachusetts, USA: Springer, Cham. Retrieved from https://cams.mit.edu/wp-content/uploads/BPS-Case-Study-03012019.pdf

Martin, A. & Eloff, J. (2002). Information security culture. In *Security in the information society: Visions and perspectives, IFIP, international conference on information security (sec2022)* (pp. 203–214). Cairo, Egypt: Kluwer. doi: http://dx.doi.org/10.1007/978-0-387-35586-3_16

Martin, G., Martin, P., Hankin, C., Darzi, A. & Kinross, J. (2017). *Cybersecurity and healthcare: how safe are we?* [Web Page]. Retrieved 2024-02-06, from https://doi.org/10.1136/bmj.j3179

Masrek, M. N., Harun, Q. N. & Zaini, M. K. (2017, 6–8 February). Information security culture for malaysian public organization: a conceptual framework. In *Proceedings of intcess 2017 4th international conference on education and social sciences* (pp. 156–166). Istanbul, Turkey. Retrieved from https://shorturl.at/cIJY0

McClure, T. (2021). *New zealand draws back from calling chinese abuses of uyghurs genocide* [Web Page]. Retrieved 2023-07-06, from https://shorter.me/JXrSo

Mendosa, D. (1994). *Tongasat's flawed genius* [Web Page]. Retrieved 2023-12-30, from http://www.mendosa.com/tongasat.html

Ministry of Health Tonga. (2019). *Introducing egovernment through digital health-tonga- project manual* (Tech. Rep. Nos. 50281–001). Nukualofa, Tonga: Government of Tonga. Retrieved from https://www.adb.org/projects/documents/ton-50281-001-pam

Mokwetli, M. & Zuva, T. (2018). Adoption of the ict security culture in smme's in the gauteng province, south africa. In *2018 international conference on advances in big data, computing and data*

communication systems (icabcd). Durban, South Africa: IEEE. doi: 10.1109/ICABCD.2018.8465139

Nasir, A., Arshah, R. & Hamid, M. (2019). A dimension-based information security culture model and its relationship with employees' security behavior: A case study in malaysian higher educational institutions. *Information Security Journal: A Global Perspective*, *28*(3), 55–80. doi: https://doi.org/10.1080/19393555.2019.1643956

Nikkei Asia. (2024). *Sri lanka's china debt trap fears grows as beijing keeps investing* [Web Page]. Retrieved 2024-03-20, from https://shorter.me/HHatL

NIST. (2019). *Glossary of key information security terms* [Web Page]. Retrieved 2023-10-01, from https://doi.org/10.6028/NIST.IR.7298r3

Nurse, J. R., Axon, L., Erola, A., Agrafiotis, I., Goldsmith, M. & Creese, S. (2020, June). The data that drives cyber insurance: A study into the underwriting and claims processes. In *2020 international conference on cyber situational awareness, data analytics and assessment (cybersa)* (pp. 1–8). Kent,UK. Retrieved from http://dx.doi.org/10.1109/CyberSA49311.2020.9139703

NZ Foreign Affairs & Trade. (2022). *China* [Web Page]. Retrieved 2024-04-06, from https://shorter.me/_gtZX

Office of the United States Trade Representative. (2018). *Findings of the investigation into china's acts, policies, and practices related to technology transfer, intellectual property, and innovation under section 301 of the trade act of 1974* [Web Page]. Retrieved 2023-03-09, from https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF

Olivos, O. (2012). Creating a security culture development plan and a case study. In *International symposium on human aspects of information security and assurance (haisa)* (p. 13-32). Crete, Greece. Retrieved from https://www.cscan.org/?page=openaccess&eid=13&id=28

Oxford English Dictionary. (2024). *Oxford english dictionary* [Web Page]. Retrieved 2024-01-18, from https://www.oed.com/

Pacific Media Centre. (2017). *Corruption in the pacific- a threat to cultural identity* [Web Page]. Retrieved 2024-01-18, from https://natlib.govt.nz/records/38892606

Pagliery, J. (2015). *The inside story of the biggest hack in history.* [Web Page]. Retrieved 2023-05-05, from https://shorter.me/7g9kj

Perry, N. (2019). *China's largesse in tonga threatens future of pacific nation.* [Web Page]. Retrieved 2023-07-11, from https://shorter.me/XGpBz

Petelo, S. (2017). *Status of e-government in tonga* [Web Page]. Retrieved 2023-05-24, from https://shorter.me/u8_pq

Peterson, D. C., Adams, A., Sanders, S. & Sanford, B. (2018). Assessing and addressing threats and risks to cybersecurity. *Frontiers of Health Services Management*, *35*(1), 23–29. doi: https://doi.org/10.1097/HAP.0000000000000040

Ponemon, L. (2016). *Sixth annual benchmark study on privacy and security of healthcare data* [Web Page]. Retrieved 2024-01-26, from https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf

Pullin, D. W. F. (2018). Cybersecurity: Positive changes through processes and team culture. *Frontiers of Health Services Management*, *35*(1), 3–12. doi: 10.1097/HAP.0000000000000038

Radio New Zealand. (2024). *Culture v corruption: Challenge for tonga's anti-corruption commissioner* [Web Page]. Retrieved 2024-01-23, from https://shorter.me/uTt_4

Radio NZ. (2007). *China set to give tonga huge loan to rebuild capital* [Web Page]. Retrieved 2023-11-18, from https://shorter.me/aNljG

Radio NZ. (2008a). *Tonga's parliament approves money for shoreline power company.* [Web Page]. Retrieved 2023-02-16, from https://shorter.me/M52tM

Radio NZ. (2008b). *Tonga's pm accuses senior civil servants of being corrupt.* [Web Page]. Retrieved 2023-01-29, from https://ln.run/bKb4r

Radio NZ. (2019). *Tonga's government backs 2006 riots investigation.* [Web Page]. Retrieved 2023-10-23, from https://ln.run/RLAJ4

Reegard, K., Blackett, C. & Katta, V. (2019). *The concept of cybersecurity culture* [Web Page]. doi: 10.3850/978-981-11-2724-3_0761-cd

Reuters. (2023). *European countries who put curbs on huawei 5g equipment.* [Web Page]. Retrieved 2023-11-19, from https://shorter.me/2fTXj

Rogers, G. (1975). *Kai and kava in niuatoputapu: Social relations, ideologies and contexts in a rural tongan community* (Unpublished doctoral dissertation). University of Auckland.

Rubenfire, A. (2017). *Building a better cyberdefence: A smarter anti-hacker dfence* [Web Page]. Retrieved 2023-01-20, from https://ln.run/8_Wpz

Ruhwanya, Z. & Ophoff, J. (2019, 21–3 May). Information security assessment of small and medium-sized enterprises in tanzania. In *International and communication technologies for development. strengthening southern-driven cooperation as a catalyst for ict4d* (pp. 776–788). Dar es Salaam, Tanzania. Retrieved from https://ln.run/6Pqwb

Runeborg, R. E. (1980). *The kingdom of tonga: History, culture and communication* (1st ed.). Honolulu, Hawaii: East West Center.

Samy, G. N., Ahmad, R. & Ismail, Z. (2010). Security threats categories in healthcare information systems. *Health Informatics Journal*, *16*(3), 201–209. doi: https://doi.org/10.1177/1460458210377468

Schein, E. H. (1996). Three cultures of management: The key to organisational learning. *MIT Sloan Management Review*, *38*(1), 9–20. Retrieved from https://ln.run/aPz99

Schwartz-Shea, P. & Yanow, D. (2013). *Interpretive research design Concepts and processes* (1st ed.). New York.: Routledge.

Scoop Media. (2006). *Shoreline press release-government of tonga.* [Web Page]. Retrieved 2023-05-22, from https://shorturl.at/dhlvG

Sengupta, K. (2017). *Isis-linked hackers attack nhs websites to show gruesome syrian civil war images 2017* [Web Page]. Retrieved 2023-06-08, from https://ln.run/9QiMw

Siponen, M. T. (2020). A conceptual foundation for organisational information security awareness. *Information Management and Computer Security*, *8*(1), 31–41. doi: https://doi.org/10.1108/09685220010371394

Sirur, S., Nurse, J. R. C. & Webb, H. (2018). Are we there yet? understanding the challenges faced in complying with the general data protection regulation (gdpr). In *In: Proceedings of the 2nd international workshop on multimedia privacy and security* (p. 88-95). Toronto, Canada: ACM. doi: https://doi.org/10.1145/3267357.3267368

Smith, C. (2018). Cybersecurity implications in an interconnected healthcare system. frontiers of health services management. *Egyptian Informatics Journal*, *35*(1), 37–40. doi: https://doi.org/10.1097/HAP.0000000000000039

Smith, R. (2023). *Revealed–how much is personal information worth on the dark web?* [Web Page]. Retrieved 2024-07-09, from https://ln.run/Q6G-9

Stack, B. (2017). *Here's how much your personal information is selling for on the dark web.* [Web Page]. Retrieved 2023-07-09, from https://ln.run/O2yYO

Swede, M. J., Scovetta, V. & Eugene- Colin, M. (2019). Protecting patient data is the new scope of practice: A recommended cybersecurity curricula for healthcare students to prepare for this challenge. *Journal of Allied Health*, *48*(2), 148–156. Retrieved from https://ln.run/uGBmK

The Commonwealth Education. (2024). *Social stratification (what it is and its systems* [Web Page]. Retrieved 2023-05-15, from https://ln.run/KNqTt

The Guardian. (2022). *China is pursuing a pacific-wide pact with 10 island nations on security, policing and data-report* [Web Page]. Retrieved 2023-07-13, from https://bitly.cx/I8xK3

The Verge. (2022). *The fcc just banned these chinese cameras and telecom hardware from reaching the us* [Web Page]. Retrieved 2024-03-22, from https://ln.run/qOSme

Tonga Parliament. (2014). *Akilisi pohiva is new pm of tonga* [Web Page]. Retrieved 2023-04-17, from https://bitly.cx/AQT

Tonga Statistics Department. (2021). *Population statistics* [Web Page]. Retrieved 2023-07-09, from https://shorter.me/FeOU1

Trevett, C. (2006). *Laughing and looting as tonga's capital burns* [Web Page]. Retrieved 2023-05-04, from https://shorter.me/ehGCR

Tully, J., Selzer, J., Phillips, J. P., O'Connor, P. & Dameff, C. (2020). Healthcare challenges in the era of cybersecurity. *Health Security*, *18*(3), 228–31. doi: https://doi.org/10.1089/hs.2019.0123

Uchendu, B., Nurse, J. R., Bada, M. & Furnell, S. (2021). Developing a cybersecurity culture: Current practices and future needs. *Computer & Security*, *109*(102387), 1–23. doi: https://doi-org.ezproxy.aut.ac.nz/10.1016/j.cose.2021.102387

United Nation Women. (2022). *Genger equality brief in tonga* [Web Page]. Retrieved 2023-03-11, from https://shorter.me/cxSa-

University of the South Pacific. (2018). *King tupou vi commissions kuku kaunaka collection* [Web Page]. Retrieved 2023-09-16, from https://shorter.me/E3npU

US Department of Health and Human Services. (1996). *Summary of the hipaa privacy rule* [Web Page]. Retrieved 2023-08-22, from https://bitly.cx/lVj

US Govt Report. (2021). *Tonga 2021 human rights report* [Web Page]. Retrieved 2024-01-15, from https://shorter.me/0xcvJ

Vakauta, K. (2017). *Tonga broadcaster saga prompts media freedom discussion* [Web Page]. Retrieved 2023-05-12, from https://shorter.me/nOyDH

von Solms, R. & Von niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*(1), 97–102. doi: https://doi.org/10.1016/j.cose.2013.04.004

Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems*, *15*(3), 320–330. doi: https://doi.org/10.1057/palgrave.ejis.3000589

Wasserman, L. & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review for the non-cyber professional. *Frontier in Digital Health*, *4*(0), 862221. doi: https://doi.org/10.3389/fdgth.2022.862221

White House Office of Trade and Manufacturing Policy. (2018). *How china's economic aggression threatens the technologies and intellectual property of the united states and the world.* [Web Page]. Retrieved 2023-02-16, from https://shorter.me/FJSXx

WHO. (2015). *The kingdom of tonga health system review* [Web Page]. Retrieved 2023-02-16, from https://shorter.me/tCBZw

WHO. (2021). *Global strategy on digital health 2020-2025* [Web Page]. Retrieved 2023-10-12, from https://shorter.me/KGfYL

WHO. (2022). *Reducing health system corruption* [Web Page]. Retrieved 2023-10-17, from https://shorter.me/NWxgQ

Williams, C. M., Chaturvedi, R. & Chakravarthy, K. (2020). Cybersecurity risks in a pandemic. *Journal of Medical Internet Research*, *22*(9), e23692. doi: https://doi.org/10.2196/23692

World Bank Organisation. (2016). *The world bank annual report 2016* [Web Page]. Retrieved 2023-02-15, from http://hdl.handle.net/10986/24985

Yeoman, S. (2021). *Waikato dhb to tell 4200 people their personal information was disclosed on the dark web, following may cyber attack* [Web Page]. Retrieved 2024-01-17, from https://shorter.me/aTk4e

Appendix A

Glossary

A.1 Acronyms

ADB Asian Development Bank.

AI Artificial Intelligent.

AMI Acute Myocardial Infarction.

BPS Banca Popolare di Sondrio.

CIA Central Intelligence Agency. (US)

CISO Chief Information Security Officers.

CPOE Computerized Provider Order Entry.

CR Cyber Resilience.

CRVS Civil Registration and Vital Statistics.

CS Cybersecurity.

CIO Chief Information Officer.

DDoS Distributed Denial-of -Service.

DoS Denial of Service.

DGSF Digital Government Strategic Framework.

DITM Drone-in-the-Middle.

EHR Electronic Health Record.

EMR Electronic Medical Record.

FBI Federal Bureau Investigation.

FDA Food and Drug Administration.

HD Hard Drive

HIPAA Health Insurance Portability and Accountability Act of 1996.

HIS Health Information System.

ICT Information Communication Technologies.

ISCCB Information Security conscious care behavior.

ISK Information Security Knowledge.

ISA Information Security Attitude.

IT Information Technology.

KISA Korea Information Security Agency.

MEIDECC Ministry of Environment, Energy, Climate Change, Disaster Management, Meteorology, Information and Communications.

MITM Man-in-the-Middle.

MoH Ministry of Health.

MOJ Ministry of Justice.

NHS National Health Service.

NIS-D Network and Information Security Directive.

OECD Organization for Economic Co-operation and Development.

OS Operating System.

PAHO Pan American Health Organization.

PLA People's Liberation Arm.

RPM Remote Patient Monitoring.

TSDF Tonga Strategic Development Framework.

UAV Unmanned Aerial Vehicles.

US United States.

WHO World Health Organisation.

A.2 Tongan terms

ako education, to learn, to study, to receive education.

anga fakafonua Traditional culture.

'api home.

'api 'a fafine home is for women.

'eiki chief, person of chiefly rank.

faa'i kavei koula The definition of the second term.

fa'e mother or mother's sister.

fafine women (plural).

fahu A fahu (father's eldest sister) is accorded the utmost respect at all formal and informal occasions, from funerals to weddings and births. She serves as the family matriarch and oversees her siblings, nieces and nephews.

faifolau navigator or voyager.

faihala to do wrong, corruption.

faikava to prepare and drink kava together with due form or ceremony. kava circle or drinking kava Tonga.

faka'apa'apa In a family or home, faka'apa'apa (respect), a value highly regarded as a Tongan koloa (treasure), is taught to children by their parents and passed on as part of their well-being and ulungaanga fakaTonga (Tongan way). life)..

fakafahafaha'i faction, taking sides in social or political context.

fakapone nepotism, is the granting of an advantage, privilege, or position to relatives or friends in a profession or field. These areas may include, but are not limited to: business, politics, science, entertainment, sports, religion and healthcare.

Falealea parliament or legislative assembly.

fale 'o e Tu'i royal household.

fangota shallow reef fishing.

fatongia role, responsibility, obligation.

felotoi concession, agreement.

fei'umu to prepare and cook or bake food in an earth oven in Tongan culture.

fei me'atokoni cooking or prepare food.

filimanako favouritism. The practice of giving unfair preferential treatment to one person or group at the expense of another..

ha'a tribe, clan. A group of people who are related or belong to the same family or bloodline. They either live together or come from the same area or city. They share the same language, culture, ancestry, history and share the same language, culture and history.

hou'eiki aristocrats, chief.

hou'eiki nopele noble, nobility, high chief.

'inasi (in ancient) presentation of food or harvest as offerings to the Tu'i Tonga or to the first lineage of kings .

kainga relatives.

kelekele land.

koloa goods, Tongan craftsmanships such as fine mats, tapa, handicrafts .

loto too compassion.

lotu religion.

mafai authority, power.

matapule chief.

monu'ia privilege, rights (ngofua), opportunity.

mamahi'i me'a to stand up for something, to fight for, to strive for.

ngatu tapa cloth made from hiapo or mulberry tree.

nofo 'a kainga managing relations with in a tribe or relatives.

popula slavery.

pule'anga government.

ta'e faka'apa'apa disrespectful.

talangofua obedience.

tapu sacred.

tauhi fanau child rearing.

tauhi va relationship.

taumalu'i fonua military defence, security, to protect.

tofi'a land estate.

tu'a a commoner, common people.

tufakanga division of labour. What is allotted to one by nature, responsibility.

tukufakaholo tradition, hereditary, handed down from generations, from predecessor to successor.

veitapui to keep away from each other. Tradition of avoidance between a brother and a sister or between cousins of the opposite gender.

'ulumotu'a head of the family or tribe.