EVALUATING POLICY LAYER SECURITY CONTROLS FOR VALUE REALISATION IN SECURE SYSTEMS

Brian Cusack; Maher Al-Khazrajy
Auckland University of Technology
{brian.cusack; maher.khazrajy} aut.ac.nz

ABSTRACT

A strategic question for any business is: What value do control frameworks give? The question concerns the costs associated with implementing and maintaining control frameworks compared with the benefits gained. Each control framework contains many controls that may or may not benefit a situation and this research is aimed at testing different selections and combinations of controls to forecast probable impacts on business outcomes. The scope of the research is limited to a representative set of security controls and the lesser question: What are the criteria for selecting the most effective and efficient security control configurations for best business value? We design a decision support tool (DSS), run a pilot study and begin to develop output sets as part of the exploratory research. The conclusion is that in controlled environments the security controls may be optimised to deliver the best business value and that the highest performing sets of controls can be forecasted once the interaction factors are known.

Keywords: Security, Controls, Performance, Business, Objectives

INTRODUCTION

A strategic question for any business is: What value do security control frameworks give? The question concerns the costs associated with implementing and maintaining control frameworks compared with the benefits gained (Barner, 2009). Each control framework contains many controls that may or may not benefit a situation and with the rapidly changing business environment many controls require improvement or retiring. A more difficult question is how to select an optimal set of security controls to control risk for the maximum value return. Often security controls are overdone and weigh as a cost to the business (Curry et al., 2006). How much security is put in place governed by the risk appetite; but the responsiveness of a control framework may be dulled by the costs, the difficulties of change management and the legacies inherited within a business culture. Many IT security risks are variant in nature – they are here for a short period of time and then the attack and vector shift. Under such conditions a security architect will add more controls than optimally necessary to create depth rather than flexibility. In a pilot study we took a set of three security controls from different published control frameworks and played different risk based games to determine the effects of a control in terms of business value. We then configured the three controls into each pair and triple combination. The results showed that principally a much larger research project is required to determine general configuration optimisation patterns under different risk based conditions but on a small pilot scale forecasting business impacts is possible from different configurations. The conclusion is that in controlled environments the security controls may be optimised to deliver the best business value and that the highest performing sets of controls can be forecasted once the interaction factors are known. The corollary is that the cost of controls can be optimised by developing responsive control frameworks that have rapid implementation and retirement schema.

IT Security advocates push to have security control frameworks and the adoption of best practice Guidelines by citing efficiency, assurance, and/or regulatory compliance (Abram, 2009). However, organizations require a clear statement of the payback value to be gained from implementing resource intensive IT control structured environments. The costs to the organization are visible in the overheads of information management, new roles, trainers, consultants, audit, and certification fees. The benefits are less visible and an organization may experience static growth and lower profit margins while IT control frameworks are being formally implemented (Fisher, 2008). Also staff commonly resent the extra "red tape" that slows the execution of business processes, slower computer responses and the sense of silly barriers to direct action. The realisation of business benefits through structured control environments may be obscured by delayed expectations and the invisibility of benefits hidden by the non-occurrence of adverse events (Kouas and Minoli, 2007). The effect is particularly apparent in security implementations. Business value has many facets, and interacting contributing factors. An assessment of the business value of IT control frameworks is a complex task that is multi-faceted and often based on subjective criteria. The intermediating layer of protection creates new behavioural

expectations for users and procedural steps that often do not translate well into the user environment. Consequently as much as the benefits of IT control frameworks have been asserted, the liability requires mitigation with tangible tools and feedback loops of measurable data to justify the expenditure (Barner, 2009).

This paper is structured to review current background literature on DSS and control frameworks. The problem of realising value from IT investments is also reviewed to elaborate the complexity of the problem context. The research set up is briefly reported and the results from the prototype computing combinations of three controls tabulated. The results are then discussed in terms of the implications for forecasting business value from other sets and configurations of IT security control variables.

CONTROL FRAMEWORKS

In the business context information technology controls are specific activities performed by people and systems to assure that the business objectives are met. Security controls are risk assessment based countermeasures to avoid, detect, counteract, or minimize the exposure of physical property, information, computer systems, and other assets. Controls help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset (Murphy, 2002). Controls are positioned in three critical phases of an event. Before the event preventive controls are intended to prevent an incident from occurring. During the event, detective controls are intended to identify and characterize an incident in progress; and, after the event, corrective controls are intended to limit the extent of any damage. Security controls hence protect an asset from value degradation while at the same time offer the opportunity for the business to take risk and to realizable return on the investment (Kounas and Minoli, 2007). A management control framework is an information structure that organizes and categorizes an organization's internal controls into clusters of risk treatments. It is designed to modify human behaviours by practices, procedures and constraints; and to modify machine utility by selecting conformance specifications that deliver the best operational outcomes. Such control frameworks come in the form of many different products designed to manage risk in different business contexts. For example, PMBOK for projects, ITIL for customer service and change management, COBIT for IT risk governance and management, and so on. The best known control framework for IT security is the ISO/IEC 27001/2 that advocates lists of specific controls for security processes and an information security management system (ISMS) (Shootreed, 2008). The governing principle behind an ISMS is that an organization should design, implement and maintain a coherent set of policies, processes and systems to mitigate failure of its information assets by assuring acceptable levels of exposure.

IT control frameworks are designed to manage risk. The elements within the frameworks provide treatments for a risk attitude an organization has developed to maintain an acceptable level of business value realisation. Risk has two attributes that contribute positively or negatively to an organization. One contribution is a cost and the other is a benefit. Every aspect of business has elements of uncertainty, and hence risk exists generally. Risk is defined as "the effect of uncertainty on objectives" (Fisher, 2008). However, organizations must have the capability to seize opportunities when they arise for growth and they must take on risks. Risk and value are two sides of the same coin. Negative Risk, however, is required to be analysed, identified, and managed to reduce the impact. It also contributes value by mitigating the occurrence of damaging events. This is where security frameworks of controls come into prevent events occurring. Risk is hence an essential part of any business and when properly managed, it drives growth and opportunity (Abram, 2009). IT control frameworks are generally applied to manage the negative aspect of risk while allowing greater opportunity for gains. Prevention and facilitation lead to a balance that optimizes the best use of risk for business value generation. IT control frameworks are published in the form of standards, best practice guides and frameworks. The International Standardization Organization (ISO) has published a wide range of standards and guidelines to regulate and advise on good practice and to help organizations achieve outcomes at a desirable quality. For example the ISO 31000:2009 - Risk management – Principles and guidelines. This International Standard consists of 11 principles and 5 attributes of excellence that establish risk management processes. ISO 27001:2013 is a risk based standard for an Information Security Management System (ISMS) that has a set of mandatory sections for every organization seeking accreditation for security conformance. In addition, there are optional sections that can be tailored to the organization's context to ensure optimum security management is in place (Shootreed, 2008). There are other control frameworks that contain security controls. For example ITIL and COBIT each have a set of security processes and mechanisms in different domains of information knowledge. In this study we selected three security controls. One from each of COBIT, ITIL and ISO/IEC 27001 to pilot test in the exploratory study the relationship between different configurations and the calculated business impact.

DESIGNING A DECISION SUPPORT SYSTEM

Decision Support Systems (DSS) are model based constructs that help a manager make decisions. Unlike an Expert System (ES) that can replace a human a DSS serves in support of a human (Bieber, 2009). As a consequence the reports are more general and the underlying computation algorithms allow for greater variation. In the past DSS have been constrained to using simulation models to compute internal and external data in relation to unstructured problems. Today DSS models are more flexible and often use game scenarios and dynamic knowledge schema for greater flexibility around complex problems. A DSS can assist by computing data that arrives at the manager's desk in large volumes and provide consistent advice. The manager also needs to learn the scope and the capability of the tool and to manage risk accordingly. Unlike an ES other forms of knowledge are required to mediate the DSS output and to make any decision align with human factors. DSS can be developed and applied to improving efficiency in many areas including control framework design and security risk management. The design of a DSS has five subsystem integrations to create the overall effect for a manager. The subsystems concern the data, the model, the knowledge, the user interface and the user (Little, 1970). Each subsystem is built and tested and then integrated and tested. In the pilot study we focused principally on the model to get the calculations performing correctly and within estimations for expected live behaviours. The results have given sufficient confidence to extend the model testing to more configurations of controls and at a later stage to build and integrate each subsystem. In the past DSS have been constrained to using simulation models to compute internal and external data in relation to unstructured problems. Today DSS models are more flexible and often use game scenarios and dynamic knowledge schema for greater flexibility around complex problems. In our build we tested a range of artificial intelligence, probabilistic and analytic algorithms to create the desired effect of a connection between a control and the business impact. None of these methods provided the consistency or the realism to be effective. At that point we then looked into different games we could play with the inputs that would deliver the required outcomes.

A further complication to resolve was the interaction between controls where one control influenced the effect of another or others. The interaction problem was complicated by the selection of controls from different control frameworks. For example if COBIT DS5 "Manage IT security Policies and Plans" security control was implemented with ISO/IEC 27001 "Information Security Policy: A.5.1.1 and .A.5.1.2; the controls have a mitigation effect on the same risk but from different perspectives. In effect there is duplication of resources at the point of overlap and it is debatable if double the expenditure on shared points of similarity result in double the impact. The interaction of controls is a complex calculation that has to be resolved by subjective investigation and approximate estimates. The point at issue is the economic effectiveness of a security control framework when interaction effects have been undervalued. The issue is accentuated when multiple frameworks are available to protect from the same risk. We found that the usual algorithm approaches for model management subsystems lacked sensitivity to chaining problems found in the multidimensional effects, of effects computation. To economically model the chains was outside of usual algorithm approaches and the potential errors in judgement that could result could outrun the usefulness of the DSS tool. Consequently we opted to play games with the controls and to optimise equilibrium points around controls and between control frameworks. In this way a best approximate could be found to a configuration condition for optimal value realisation.

THE FINDINGS

The DSS tool was built using successive and regressive phases of the Design Science framework (Hevner, et al, 2014). For this reported phase of the research only the model management subsystem was developed and as further refinements and generalisations are made from these results the other four subsystems will be built and integrated. Design Science (DS) is an organising framework and philosophy for making and building artefacts. It has been made relevant to Information Systems (IS) and Information Technology (IT) research as a methodology and in this research it is applied to making a new and improved DSS tool (Hevner, et al., 2004; Nunamaker, et al., 1990; Goes, 2014). The benefit of the approach is that a tool may be investigated in context and improved through continuous iterations and testing (Walls, et al., 2004). The purpose of the DS research methodology is to answer research questions through the artefact and its actions. Depending on the characteristics and the goals of the research, a researcher can shape the processes to deliver innovative or confirmatory outcomes (Johannesson and Perjons, 2014). The DS research methodology consists of six main phases: problem identification and motivation, define the objectives for a solution, design and development, demonstration, evaluation and communication (Peffers, et al., 2007, p.54). It has four entry points for starting research and six phases that are linked by output loops and feedback loops. The consequence is that

any action that is taken is balanced by evaluation and the outcome of the evaluation can deliver forward propagation to the next phase or a return to an earlier phase for improvement.

The DSS Tool model management subsystem was constructed in Excel to analyse risk impacts based on likelihood and calculated game plays. The generated digits are summarised into a cumulative impact distribution. A pilot test was conducted with the proto-type DSS that describes the distribution for the cumulative impact of C0, C1, and C2 respectively. C0 was a single security control taken from the control framework COBIT; C1 was two controls one COBIT and one from the ITIL control framework; and C2 was three controls – one from COBIT, one from ITIL and one from ISO/IEC 27001 control framework. All controls concerned security access control and are generalised for the calculations. As shown in Table 1, there are three risks R1, R2 and R3, and the likelihood rating of these risks can be L (low), medium (M) or high (H). For a given control configuration Cn:

a. the probability distribution for risk R1 lists possible values of R1 and the assumed probabilities (likelihood) e.g. pr(R1=L)=0.1, pr(R1=M)=0.4, pr(R1=H)=0.5

b. there are a set of assumed impact levels categorised as 0, 1, 2, 3, 4 or 5 where low is beneficial.

The impact levels are obtained from game play and are a summary of the results of that staged interaction. The cost of implementation is also reported based on an estimated cost for each control and condition. There are two rows for probabilities as shown (pr, pr adj). It can be seen that values of 1, 2, 1 to set to the likelihood rate M is twice as likely as L or H. Assumed probabilities (likelihood) ratings are entered in row 9. The second probability row (pr adj) adjusts the entered numbers so that the set of probabilities all adds to 1. The impact of each risk level for each risk is entered in row 5 e.g. if R1 is L the impact is 3, if R1 is M the impact is 4 and if R1 is H the impact is 5. Similarly, for another control configuration C1. The cost, probability and impact information is entered in respective rows. If a probability or impact differs from that entered for C0 the entry is automatically reported in bold so a comparison can be made. Similarly, for control configuration C2.

Table 1. Control Configuration Cost and Associated Risks

		R1	r1L	r1M	r1H			R2	r2L	r2M	r2H			R3	r3L	r3M	r3H	
C0	10																	
1		pr	0.20	0.40	0.50	1.1		pr	1.00	3.00	2.00	6.0		pr	1.00	2.00	1.00	4.0
2		pr adj	0.18	0.36	0.45	1.0		pr adj	0.17	0.50	0.33	1.0		pr adj	0.25	0.50	0.25	1.0
3		impact	3	4	5			impact	1	3	5			impact	2	3	4	
C1	15	cost																
1		pr	0.20	**0.50**	**0.20**	0.9		pr	1.00	**2.00**	**0.50**	3.5		pr	**1.50**	2.00		3.5
2		pr adj	**0.22**	**0.56**	**0.22**	1.0		pr adj	**0.29**	**0.57**	**0.14**	1.0		pr adj	**0.43**	**0.57**		1.0
3		impact	**1**	**3**	**4**			impact		**2**	**4**			impact	**1**	**2**	4	
C2	25																	
1		pr	**0.40**	0.40	**0.20**	1.0		pr	1.00	3.00	**1.00**	5.0		pr	**3.00**	2.00	1.00	6.0
2		pr adj	**0.40**	**0.40**	**0.20**	1.0		pr adj	**0.20**	**0.60**	**0.20**	1.0		pr adj	**0.50**	**0.33**	**0.17**	1.0
3		impact	**1**	**3**	**4**			impact	1	**2**	**3**			impact	2	3	4	

In Figure 1 the impacts are reported for C0 to illustrate the DSS effect for discussion (and to stay in the word limit). Figure 1 has two charts within that show the distribution and the cumulative impact respectively. In chart 1 the risk and realisation are shown to cluster and imprint around a central value. It is clear that this security control has no impact on a number of risks but is effective for approximately five. The chart 2 reports the cumulative impact distribution and shows the risk range for which the treatment is most effective. To generalise the result we expect to show the effectiveness of each control and where overlapping control impacts can be resolved to treat a risk economically.

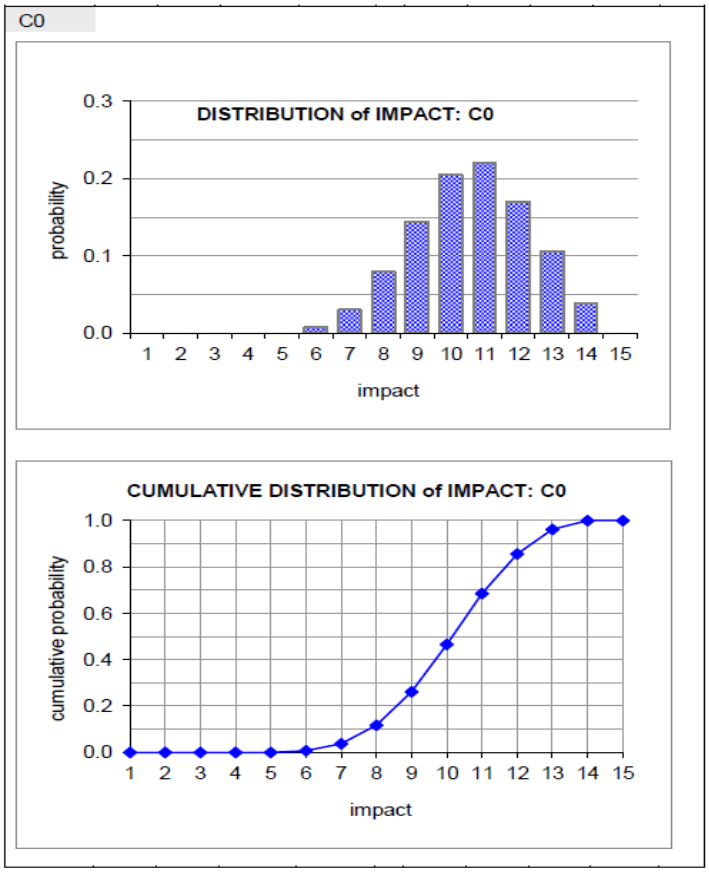

Figure 1. Risk-Impact Analysis

DISCUSSION

The results suggest that the pilot study for three security controls from commonly used frameworks can be computed within the game play to deliver useful business impact estimates. The realisation of business benefits from the implementation of IT control frameworks is asserted to be a trade-off of positive and negative risk treatment; and is controlled by many variables interacting in the delivery of outcomes. An organization implementing IT control frameworks undertakes an exercise that is both potentially rewarding and costly at the same time. Our results show that these metrics can be consistently estimated for different controls and control configurations. The ongoing debate in most businesses is the quantification of qualitative and subjective business gains, and how to represent qualitative risk in monetary terms. The overall quality of the assessment process around the management of risk ultimately determines the success or otherwise of a decision. A poor decision-making process results in either taking a highly assertive attitude for the loss of business opportunities or making daring undertakings that could result in adverse consequences. Either way, the business loses. On the contrary, if IT risks are adequately assessed and controls are proportionally selected, then, prioritising controls and subsequent validation testing is budgeted accordingly. Control costs do not vary often and when they do, it can be approximated, for example, increased licence fees for antivirus or the cost of extra firewall appliances, hiring another system administrator to the network team. However, risk impact and likelihood of the risk to materialise could change more frequently and in unpredictable patterns. The exploratory research to develop a DSS to support security managers allows flexible inputs, changes in game rules and alteration of risk estimates in changing circumstances.

The distribution impact of C0 is expected to be found from other controls and from controls in other control frameworks, but in each instance the distribution is forecasted to be different. The difference may be as great as independence and as close as similarity. In one control framework such as ISO/IEC 27001 it is expected the overlap between related controls is minimal. As a network (or framework) of controls then the overall impact distribution ought to cover the scope of a risk context evaluation and provide information so that informed decisions can be made. The type of decisions would include a trade of costs, risk appetites and the forecast of an expected financial return. The tool can hence optimise the number and type of controls selected to meet outcome expectations and budget expenditure. In the case of controls being selected from multiple frameworks then our example shows similarities between controls in terms of the treatment of risk. Consequently the question of financial optimisation can be addressed again by eliminating similar treatments for the same risk and selecting a single control and one cost for the forecasted return. For example many organisations opt to mix controls from COBIT for management layer security and ITL for operations layer security, but the DSS trial shows that a single ISO/IEC 27001 control may be more effective.

The limitation of the research is its exploratory nature and the pilot trial on three security controls. Businesses expect that the IT investment can be tailor made to be responsive to budgets and to deliver the required protection at a minimal cost. In the research we restrict the scope to three different well known control frameworks but there are many more. The focus of this research is on IT control frameworks that are generally applied to manage the negative aspect of risk and have left the balancing task to the security manager. Further research can be extended to include the optimisation of game play and the games played in different circumstances. The flexibility we have shown also has to be tested under different circumstances. This requires the alteration of estimates in response to fresh risk evaluations and the evaluation of the DSS against expected performances. Risk contexts change over unpredictable time bases and the DSS is expected to be responsive to new calculations at any time. There are always changes in regulations and competition but the rate of change in technology capability and use is a major driver for re-assessing risk profiles. Flexibility in the creation of and the adjustment of IT controls facilitate the durability of an assurance framework. Consequently in our research we have attempted to bridge the differences between IT pragmatic practices and business numerical rational expectations by constructing the beginnings of a decision support tool (DSS) to assist the aligning of IT decision-making with business outcome forecasts.

CONCLUSION

The exploratory research has reduced a much larger problem to the theoretical testing of three security controls and a forecast of estimated business impacts. The prototype is a proof of concept that shows this type of research is feasible and the typical highly subjective adoption of security control frameworks can proceed with the help of a moderating DSS. Such DSS can manage the processing of the large and repetitive data sets required to adequately calculate the interaction between controls in and for different contexts. The criteria for selecting control configurations can thus be flexible in relation to the required business outcomes and costs optimised for the best value realisation.

REFERENCES

Abram, T. 2009. “The Hidden Values of IT Risk Management.” *ISACA Journal*. (2), 52-56.

Barneir, B. 2009. “Driving Value From Nonrevenue-generating Activities: Myths and Misunderstandings of Governance and Risk Management.” *ISACA Journal*. (2), 37-43.

Bieber, M. 1995. On integrating hypermedia into decision support and other information systems. Decision Support Systems, (14:3), 32-42.

Curry, A., Flett, P., and Hollingsworth, I. 2006. Managing Information and Systems: The Business Perspective. London: Routledge, 2006.

Fischer, U. 2008. “New Framework for Enterprise Risk Management in IT”. *ISACA Journal*. (4), 22-23

Goes, P. 2014. “Design Science Research Top Information Systems Journals” *MIS Quarterly* (38:1) iii-viii.

Hevner, A., March, S., Park, J. and ram 2004. “Design science in information system research”, *MIS Quarterly* (28:1), 75-105.

Johannesson, P., & Perjons, E. 2014. “A Method Framework for Design Science Research”. In An Introduction to Design Science 75-89. Switzerland: Springer.

Kouns, J., Minoli, D. 2007. Information Technology Risk Management in Enterprise Environment. Wiley-Interscience.

Little, J. 1970. Models and Managers: The concept of decision calculus. *Management Science*, (16:8), 17-28.

Murphy, T. 2002. Achieving Business Value from Technology: A practical guide for Today's Executive. N.J: John Willey & Sons, Inc.

Nunamaker, J., Chen, M. and Purdin, T. 1990. "Systems development in information systems research". *Journal of Management Information Systems* (7:3), 89-106.

Peffers, K., Tuunanen, T., Rothenberger, M. and Chatterjee, S. 2007. "A Design Science Research Methodology for Information Systems Research". *Journal of Management Information Systems*, (24:3), 45-77.

Shootreed, J. 2008. "Risk Management best practice is ISO 31000."http://www.irr-neram.ca/pdf_files/May9-2008/shortreed.pdf