BC3I – TOWARDS REQUIREMENTS SPECIFICATION FOR PREPARING AN INFORMATION SECURITY BUDGET

MT Dlamini[1], MM Eloff[2], JHP Eloff[1,3], K Hone[1]

[1]Information and Computer Security Architectures Research Group

Department of Computer Science, University of Pretoria, South Africa

[2]School of Computing, UNISA, Pretoria, South Africa

[3]SAP Meraka UTD, CSIR, South Africa

{[1]mdlamini, [3]eloff}@cs.up.ac.za, Tel.:+27129999100

[2]eloffmm@unisa.ac.za, Tel.:+27124296336

[1]KarinH@tebabank.com Tel.: +27115185619

ABSTRACT

The entire business landscape finds itself on the verge of a recession because of ongoing global economic turmoil. Thus, there is a heightened need to minimise and mitigate business risk and scrutinise information spending while ensuring compliance with regulatory mandates. This calls for decision makers to become vigilant in their spending and move towards an optimised information security investment. The main aim of this paper is to provide decision makers with a set of requirements to be considered when implementing a cost-effective and optimal information security budget; in a manner that preserve organisations' information security posture and compliance status. Research reported on in this paper forms part of an ongoing project known as the BC3I (Broad Control Category Cost Indicators) framework.

KEY WORDS

Information security spending, requirements, controls, economics, information security breaches, regulatory compliance.

1 INTRODUCTION

Information security is a continuously changing discipline that requires continuous adaptation to new and ever-changing information security threats, countermeasures and the global business landscape. The global business landscape is on the verge of facing a recession following the ongoing global economic turmoil. This came as a result of the collapse of the United States of America's sub-prime mortgage market (Kiviat, 2009). Organisations must quickly adapt to the prevailing economic climate by becoming more vigilant in their spending in general and more so on overheads such as information security expenditure (Researchandmarkets, 2007; Tipton & Krause, 2003; Timms, 2004).

Alas, despite the lingering global economic turmoil and encouraging developments in information security, a survey conducted by Symantec late last year (2008) revealed that the global underground economy is booming at millions of dollars in advertised goods and services (Symantec, 2008; Ko, 2008). While the whole world is in the worst economic crisis, the underground economy continues to flourish.

Despite all the years of hard work on information security technology improvements, harsh compliance regulatory penalties and more coordinated law enforcements, information security breaches are still ubiquitous and have seriously damaging consequences (Grossklags, Chuang & Christin, 2008; Fumey-Nassah, 2007; Schneier, 2002). Clearly, something is not working effectively in the information security arena.

Are the organisations putting in enough effort to protect their information assets or are they not taking any precautions? Is it too little or just enough or more? How much is really enough? This paper investigates the requirements to provide input for the preparation of a budget for information security. Research done in preparation of this paper is part of an ongoing project known as the BC3I framework (Broad Control Category Cost Indicators) (Dlamini, Eloff & Eloff, 2009).

The remainder of the paper is structured as follows: Section 2 gives a brief background on the economics of information security; Section 3 discusses related work on information security investment; Section 4

discusses the requirements to be considered when implementing a cost effective information security, and Section 5 concludes the paper.

2 RELATED WORK

The field of economics of information security has become an important field of study (Tsiakis & Stephanides, 2005; Huang, Hu & Behara, 2006; Anderson & Moore, 2006; Anderson & Moore, 2007). For the past seven years, researchers have identified several topics of interest but this paper focuses only on **the economics of information security investment** (Gordon & Loeb, 2002; Camp, 2006; Anderson & Moore, 2006; Grossklags, Christin & Chuang, 2008; Hulthen, 2008).

The related literature investigated for this research project is structured as follows:

- A brief overview of the field of the economics of information security investment.
- Optimal allocation of resources to information security activities, with specific reference to the work of Gordon and Loeb (2002).

2.1 The Economics of Information Security Investment

This paper focuses on the topic of information security investment which is viewed from two opposing perspectives: either from the system defender's or the attacker's point of view.

Investing in information security is a trade-off; organisations can either choose to invest in security or not to invest (Anderson, 2001; Ioannidis, Pym & Williams, 2009). There are both direct and indirect benefits and costs involved. Directly, investing in information security reduces the risk exposure – though at an opportunity cost of other profitable investment. Not investing in information security guarantees more money – but at an opportunity cost of not having secure information assets. Indirectly investing in information security can help those who have not invested to "a free ride". Those who do invest, could easily become victims of threats that come from those who fail to invest (what economists call externality). Information security practitioners have to consider the trade-offs and related issues when they scrutinise and make information security investment decisions.

Given the current threat landscape, the consequences of not investing in information security can prove to be more costly than the consequences of investing (Fumey-Nassah, 2007). Chapman (2009) highlight that organisations are losing billions of dollars because of information security breaches. The amount of time and effort that is involved in recovering from an information security breach, besides compliance fines and penalties to be paid is also a cause of concern. Over the years, organisations have therefore been left with no option but to invest in information security.

2.2 An Optimal Allocation of Funds to Information Security

Organisations need adequate information security at a reasonable cost. For information security to make business sense; organisations must strike the right balance between the likelihood of risk and the cost to reduce such risk (Su, 2006). This has proven not an easy task to do. Goetz and Johnson (2006) point out that a majority of executives view information security as a "bottomless pit that never gets full" and some see it as "necessary evil that hinders productivity" (Conray-Murray, 2003). This is mainly due to the failure of information security managers to quantify their expenditure and the likelihood of the risk, faced by the information assets materialising. This failure has led executives to ask "how much is really enough for information security?"

In answering the fore-going question and contrary to the views of "a bottomless information security pit that never gets full"; researchers argue that there is actually an optimal point for information security spending (Anderson, 2001; Huang, Hu & Behara, 2008) which several researchers have tried to determine. It is not advisable to invest below or beyond this point.

Huang et al. (2006) use an economic model to determine optimal information security spending for organisations under multiple attacks. Modelling with variables such as system vulnerability, potential loss, budget and investment effectiveness, they demonstrate how to optimally allocate information security investments.

Wang and Song (2008) propose modelling with information security requirements, opportunity costs of the risks and budget constraints. They use a multi-objective decision-making framework to determine the

optimal information security investment. Unfortunately, the modelling approaches discussed in both Huang et al. (2006) and Wang and Song (2008) do not provide a definite figure or the exact point of optimality for an information security investment. Srinidhi et al. (2008) also present a model to assist information security managers to optimally allocate financial resources to information security so as to guarantee productivity and the safety of information assets.

In 2002, Gordon and Loeb proposed an economic model (G&L model hereafter) to determine the optimal allocation of funds among different assets with different vulnerabilities to information security. Unlike the work of Huang et al. (2006) and Wang and Song (2008), their findings show that the optimal investment for protecting an information asset must at least be less than or equal to 37% of the total loss expected of the information asset. Willemson (2006) reviewed and refuted the G&L model's claim. Relaxing this model's assumptions, Willemson provided a function that suggests an investment of up to 50% and even up to 100% of the expected loss of an information asset.

Tanaka, Matsuura and Sudoh (2005) subsequently conducted an extensive empirical study using the G&L model. Their work investigates the relationship between information sharing and vulnerability levels and how it influences the decisions on information security investments. Liu et al. (2007) also conducted an empirical study on the G&L model to verify the relationship between the effects of an information security investment and the vulnerability level. Matsuura (2008) remarks that the G&L model derive it's economic benefit from threat reduction, but concludes that this is not sufficient. Therefore Matsuura extended the G&L model to include a measure of productivity.

Huang et al. (2008) have since extended the G&L model to include a risk-averse decision maker instead of a risk-neutral decision maker and adopted the expected utility theory. They have modelled the relationship between potential loss, the extent of risk aversion and the effectiveness of an information security investment. The majority of the work done seems to concentrate on how much to invest in information security. However, several important shortcomings still exist as pointed out in the next paragraph.

2.3 Recommendations drawn from the reviewed literature

The problem with the current body of knowledge is that it does not provide or recommend a set of requirements that decision makers have to consider when they develop their budgeting models. Requirements can act as a bridge in attempting to solve the problem of optimal resource allocation for information security.

Furthermore, decision makers need to provide evidence of the success of their information security spending. Due to the difficulty in establishing the monetary value of information security benefits, requirements can also be used to act as the measure of success or failure of models for the allocation of resources.

Requirements elicitation is therefore an acceptable departure point in the attempt to find solutions to the optimal and effective allocation of funds for information security.

3 REQUIREMENTS

The need for efficient and effective budgeting and spending on information security is driven by a number of different high-level requirements, ranging from technological to strategic issues. The elicitation of requirements for preparing an information security budget as proposed in this paper is structured as follows:

3.1 Requirements gleaned from existing approaches

3.2 Additional requirements

3.1 Requirements gleaned from existing approaches

The following list of requirements was identified from literature as referenced in this paper:

- Information security should be viewed as a multi-disciplinary field and therefore the budget should reflect implementation issues across the spectrum of people, process and technology.
- The budget should reflect implementation issues on the defence as well as attack side, i.e. proactive versus reactive.
- Careful consideration should be given to striking a balance between following a “standard-of-due-care” approach and following an approach based on risk assessment.

- An information security budget should address more than merely regulatory and standards compliance.

An information security budget should be based on assumptions clearly communicated to senior management, with specific reference to the % coverage of vulnerability exposure as well as the % acceptable risk levels.

3.2 Additional Requirements

The authors of the paper in hand have identified the following additional requirements to be considered when preparing a budget for information security:

3.2.1 Taking cognisance of the three organisational levels

3.2.2 Compiling and using a well-defined Information Security Architecture

3.2.3 Other non-functional requirements

3.2.1 Taking cognisance of the three organisational levels

Cognisance has to be taken of the three well-known organisational levels, namely strategic, tactical and operational. These levels are to be used as a framework for organising the proposed requirements (Rolfsdotter Karlsson, 2008).

3.2.1.1 Strategic Level

On the strategic level, the budget for information security should be aligned with the vision and mission statement of the organisation, the business goals, legal obligations, overall risk appetite and policy statements. Any money spent should be in direct support of realistic and reachable business goals and priorities of the organisation. The business goals are derived from the vision, mission and values that are translated into the critical success factors of the organisation (Rolfsdotter Karlsson, 2008). This ensures that information security programmes are tightly coupled to the overall business strategy.

Legal obligations are stipulated in national and international regulatory requirements and laws. Organisations are forced to adhere to these or face prosecution if they do not.

Industry related laws and regulations must also be taken into account. Policy documents may also confirm the intent of an organisation, for example to protect the privacy of third parties. A policy describes the specific steps that an organisation will take and expects its employees to adhere to these in order to reach the organisation's business goals.

3.2.1.2 Tactical Level

The tactical level includes risk analysis for the identification of threats; standards and any compliance requirements. Thus it plays an important role in identifying threats to the security of information assets. It plays a guiding role in deciding 'how much' to spend on 'what'. Butler (2003) identifies a number of shortcomings of risk analysis, such as that exact investment decisions have to be made based on 'guesstimated' information.

Compliance with international standards also influences the spending on information security. Many countries have equivalent standards on national level that reflect ISO/IEC 27002, such as the British Standard BS ISO/IEC 27002:2005 and the AS/NZS ISO/IEC 17799:2006 standard in New Zealand and Australia.

3.2.1.3 Operational Level

On the operational level, both operational and technological requirements need to be considered. Operational requirements include aspects such as affordability of manpower, resources, optimal protection levels and feasibility. Furthermore, the operational level includes administrative requirements referring to guiding the user's actions to meet business goals and objectives as specified on the strategic level.

Technological requirements include both ICT infrastructure components such as controls on the hardware and software levels. When selecting controls, identification of an optimal mix of controls is of vital importance.

3.2.2 Compiling and using a well-defined Information Security Architecture

Eloff and Eloff (2005) proposed a number of requirements for the establishment of an information security architecture. These requirements – originally defined for developing information security architecture – can

also be translated into requirements for information security budgets. The requirements state that information security architecture should

- **be holistic and encompassing**: The budget for information security should indeed be holistic and refer to the full spectrum of controls to be implemented. The requirement of holism involves the inclusion of all aspects when budgeting for security. the budget should not focus on isolated aspects but on all aspects.
- **make suggestions on how different controls can be synchronised and integrated to achieve maximum effect**: Very few organisations today spend enough time on the synchronisation and integration of controls, resulting in a potential over expenditure and duplication of controls. The synchronisation and integration of controls in most cases are organisation specific.
- **include a comprehensive approach to information security risk management**: The relationship between a comprehensive approach towards risk management and the information security budget is self-explanatory as the budget for information security should very clearly indicate how much risk mitigation is planned for, as well as the acceptable risk that the organisation will endure.
- **be measurable to demonstrate adherence to the requirements as set out**. Research has shown that it is somehow difficult to establish the monetary value of information security controls and of the benefits derived (Abrams et al., 1998; Conrad, 2005; Pfleeger & Pfleeger, 2007; Srinidhi et al., 2008). Despite these difficulties, the results should be expressed in monetary terms.

3.2.3 Other non-functional requirements

Non-functional requirements are viewed as those that impose constraints on the compilation of the budget for information security. Previous work done by the authors of this paper, as reported in Dlamini et al. (2009), suggest the following high-level non-functional requirements:

- **Flexibility**: This requirement recognises the fact that organisations are different and that they exist in different sectors. One prescribed solution regarding information security controls will not satisfy the requirements of all organisations.
- **Cost effectiveness:** Organisations must be able to identify and implement those controls that will protect their information resources

in the most cost-effective way. Implementing all the controls may be a matter of “overkill”, thus just “enough” should be implemented.

Lastly, the existing and current information security budget must not be ignored as a valuable input into future budget definitions. The existing budget will also shape where recurring costs must be budgeted for, e.g. licensing fees on information security tools, hardware upgrades on information security technology.

3.3 SUMMARY

In a nutshell, the UML diagram depicted in Figure 1 is used to model the requirements for preparing an information security budget as proposed in this paper.

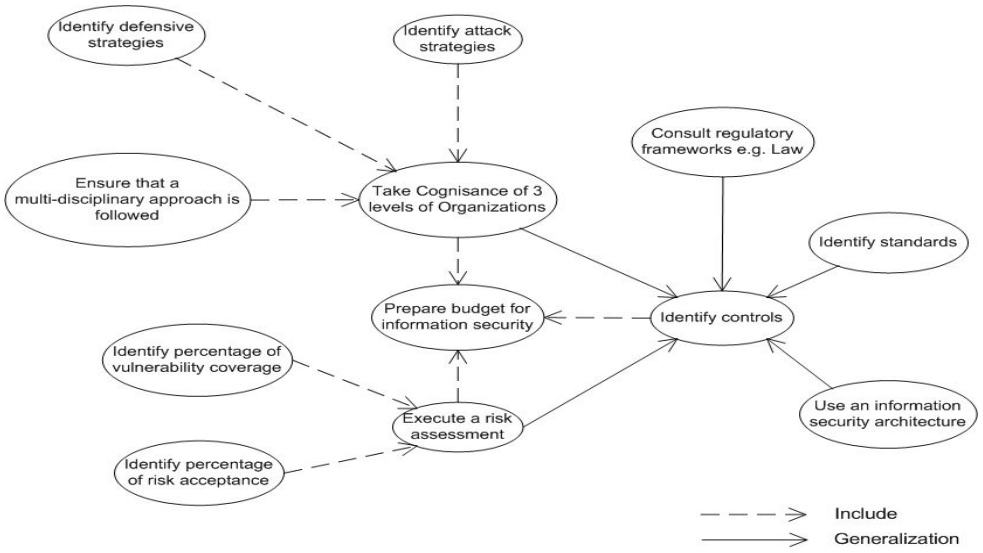

Figure 1: Use case and collaboration diagram for preparing an information security budget

Consider the above diagram. The identification of controls can be generalised as being the output of activities such as controls identified by means of regulatory investigations, standards, use of information security architecture, risk analysis, as well as cognisance of the three organisational levels. These generalisations are depicted by fixed lines whereas the broken lines show activities that should be included in the activity when preparing a budget for information security.

4 CONCLUSION

The current economic crisis is affecting organisations world-wide and all are required to spend money wisely. This also applies to spending on information security. Current models and approaches to determine *how much* to spend on *what* in order to safeguard information assets do not consider the total picture of an organisation and the environment in which it operates? In this paper the authors approached this problem holistically and identified the requirements to be considered when preparing an information security budget. These requirements are presented in a "use case" diagram that illustrates the potential interaction between the different components.

Acknowledgments:

The support of SAP Research CEC Pretoria towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at are those of the authors and cannot necessarily be attributed to SAP Research.

5 REFERENCES

Abrams, M.D., Johnson, C.M., Kahn, J.J. and King, S.G. (1998) Considerations for Allocating Resources for Information Security. Available online at www.c4i.org/caris.pdf, accessed on 09 February 2009.

Anderson, R. (2001) Why Information Security is Hard – An Economic Perspective, the *17th Annual Computer Security Applications Conference*, 10 - 14December 2001, New Orleans, Louisiana, USA.

Anderson, R. and Moore, T. (2006) The Economics of Information Security, *Science* 314(5799): 610-613, 27 October 2006.

Anderson, R. and Moore, T. (2007) Information Security Economics – and Beyond. Available online at: http://www.cl.cam.ac.uk/~rja14/Papers/econ_crypto.pdf, accessed on 12 January 2009.

Butler, S.A. (2003) Security Attribute Evaluation Method, PhD Thesis, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA 15213, USA.

Camp, L.J. (2006) The state of Economics of Information Security, *I/S: Journal of Law and Policy*, 2(2): 189-205.

Chapman, G. (2009) Cybercrime losses top $US1 trillion. Available online at: http://www.australianit.news.com.au/story/0,24897,24997483-24169,00.html, accessed on 19 February 2009.

Conrad, J.R. (2005) Analyzing Risks of Information Security Investments with Monte-Carlo Simulations, *Fourth Workshop on the Economics of Information Security*, 2-3 June 2005, Kennedy School of Government, Harvard University.

Conray-Murray, A. (2003) Strategies & issues: justifying security spending. Available online at: http://www.itarchitect.com/articles/NMG20020930S0002.html; accessed on 18.July 2007.

Dlamini, M.; Eloff, J.H.P. and Eloff, M.M. (2009) BC3I – A Model for Information Security Cost Indicators, submitted to the *Journal of Research and Practice in Information* Technology.

Eloff J.H.P. and Eloff M.M. (2005) Information Security Architecture, *Computers Fraud & Security*, 2005(11): 10-16, Nov 2005.

Fumey-Nassah, G. (2007) The Management of Economic Ramification of Information and Network Security on an Organization, *Proceedings of the Information Security Curriculum development Conference '07*, 28 – 29 September 2007, Kennesaw, Georgia, USA.

Goetz, E. and Johnson, M.E. (2006) Embedding Information Security Risk Management into the Extended Enterprise: An Executive Workshop, *MacNamee Center for Digital Strategies*, Tuck School of Business at Dartmouth University, USA. Available online at http://mba.tuck.dartmouth.edu/digital/Programs/CorporateEvents/CIO_RiskManage/Overview.pdf, accessed on 18 February 2009.

Gordon, L.A. and Loeb, M.P. (2002) The Economics of Information Security Investments, *ACM Transactions on Information and System Security*, (5)4: 438-457, November 2002.

Grossklags, J., Chuang, J. and Christin, N. (2008) Security Investment (failures) in Five Economic Environments: A Comparison of Homogeneous and Heterogeneous User Agents, *The Seventh Workshop on the Economics of Information Security*, 25 -28 June 2008, The Center for Digital Strategies, Tuck School of Business at Dartmouth College, Hanover, USA.

Huang, C.D., Hu, Q. and Behara, R.S. (2006) Economics of Information Security Investment in the Case of Simultaneous Attacks, *The Fifth Workshop on the Economics of Information Security (WEIS 2006)*, 26-28 January 2006, Robinson College, University of Cambridge, England.

Huang, C.D., Hu, Q. and Beraha, R.S. (2008) An Economic analysis of the optimal information security investment in the case of a risk averse firm, *The International Journal of Production Economics*, 2008(114): 793 - 804

Hulthen, R. (2008) Communicating the Economic Value of Security Investment: Value at Security Risk, *The Seventh Workshop on the Economics of Information Security*, 25-28 June 2008, Hanover, USA.

Ioannidis, C., Pym, D. and Williams, J. (2009) Investments trade-offs in the Economics of Information Security, *the thirteenth Proceedings of the conference of Financial Cryptography and Data Security*, 23 – 26 February 2009, Barbados, USA.

ISO/IEC 27002:2005, July 2007 *Information technology - Security techniques - Code of practice for information security management*, renumbered in 2007.

Kiviat, B. (2009) How to Fix the Housing Market, Times Magazine. Available online at: http://www.time.com/time/magazine/article/0,9171,1879184-2,00.html, accessed on 19 February 2009.

Ko, C. (2008) Underground Economy Booming Online, Says Symantec, IDG News Service. Available online at: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9123142&source=rss_ind130, accessed on10 January 2009.

Liu, W., Tanaka, H. and Matsuura, K. (2007) Empirical-Analysis Methodology for Information-Security Investment and Its Application to Reliable Survey of Japanese Firms, Regular Paper, *IPSJ Digital Courier*, 3: 585 – 599.

Matsuura, K. (2008) Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model, *The Seventh Workshop on the Economics of Information Security*, 25-28 June 2008, Hanover, USA.

Pfleeger, C.P. and Pfleeger, S.L. (2007) *Security in Computing*, 4th edition, Pearson Education, Inc, United States.

Researchandmarkets (2007) IT Security Market Report 2007, UK. Available at: http://www.bharatbook.com/productdetail.asp?id=11035, accessed [18 February 2009]

Rolfsdotter Karlsson, A., (2008) *Managing Performance Measurement: A study of how to select and implement performance measures on a strategic, tactical and operational level*, Master's Thesis, University of Gävle, Sweden.

Schneier, B. (2002) Computer Security: It's the Economics, Stupid, 1st Workshop on the *Economics of Information Security*, 16 -17 May 2002, University of California, Berkeley, USA.

Srinidhi, B., Yan, J. and Tayi, G.K. (2008) Firm-level Resource Allocation to Information Security in the Presence of Financial Distress, *Working paper Series 2008-17*, School of Economic Sciences, Washington State University, USA. Available online at www.ses.wsu.edu/PDFFiles/WorkingPapers/Yan/Srinidhi_Yan_GiriJune2008MISQ.pdf, accessed on 09 February 2009.

Su, X. (2006) An Overview of Economic Approaches to Information Security Management, Technical Report TR-CTIT-06-30, *Centre for Telematics and Information Technology*, University of Twente, Information Systems Group, Enschede, ISSN 1381 – 3625, Netherlands.

Symantec (2008) Symantec Report on the Underground Economy (July 2007 – June 2008), Whitepaper. Available online at: eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf accessed on 09 January 2009.

Tanaka, H., Matsuura, K. and Sudoh, O. (2005) Vulnerability and Information Security Investment: An Empirical Analysis of e-local Government in Japan, *Journal of Accounting and Public Policy*, Elsevier, 2005(24): 37-59.

Timms, S. (2004) Information Security Breaches Survey 2004: Executive Summary, PriceWaterhouseCoopers, Department of Trade and Industry, UK. Available online at: http://www.entrust.com/resources/pdf/ukdti_infosecbreachessurvey2004_execsumm.pdf, accessed on 18 February 2009.

Tipton, H.F. and Krause, M. (2003*) Information Security Management Handbook, 5th Edition*, Auerbach Publication, New York, USA.

Tsiakis, T. and Stephanides, G. (2005) The Economic Approach of Information Security, *Computers & Security*, 24(2): 105-108.

Wang, Z. and Song, H. (2008) Towards an optimal information security investment strategy, *IEEE Conference on Networking, Sensing and Control 2008*, April 6 – 8, 2008, pp. 756 – 761.

Willemson, J. (2006) On the Gordon and Loeb Model for Information Security Investment, presented at *The Fifth Workshop on the Economics of Information Security* (WEIS 2006), University of Cambridge, UK, 26-28 June 2006. Available online at http://www.ut.ee/~jan/publ/economics.ps, accessed on27 November 2007.