The current issue and full text archive of this journal is available on Emerald Insight at:
https://www.emerald.com/insight/1750-6166.htm

Optimum spending on cybersecurity measures

Tara Kissoon
Henley School of Business, University of Reading Henley Business School – Greenlands Campus, Henley-on-Thames, Oxfordshire, UK

Received 19 November 2019
Revised 3 February 2020
13 March 2020
Accepted 1 April 2020

Abstract

Purpose – This purpose of this paper is to provide insight through analysis of the data collected from a pilot study, into the decision-making process used by organizations in cybersecurity investments. Leveraging the review of literature, this paper aims to explore the strategic decisions made by organizations when implementing cybersecurity controls, and identifies economic models and theories from the economics of information security, and information security investment decision-making process. Using a survey study method, this paper explores the feasibility for development of a strategic decision-making framework that may be used when evaluating and implementing cybersecurity measures.

Design/methodology/approach – A pilot study was conducted to evaluate the ways in which decisions are made as it relates to cybersecurity spending. The purpose of the pilot study was to determine the feasibility for developing a strategic framework to minimize cybersecurity risks. Phase 1 – Interview Study: The qualitative approach focused on seven participants who provided input to refine the survey study questionnaire. Phase 2 – Survey Study: The qualitative approach focused on information gathered through an online descriptive survey study using a five-point Likert scale.

Findings – The literature review identified that there is limited research in the area of information security decision making. One paper was identified within this area, focusing on the research completed by Dor and Elovici [22]. This exploratory research demonstrates that although organizations have actively implemented cybersecurity frameworks, there is a need to enhance the decision-making process to reduce the number and type of breaches, along with strengthening the cybersecurity framework to facilitate a preventative approach.

Research limitations/implications – The partnership research design could be expanded to facilitate quantitative and qualitative techniques in parallel with equal weight, leveraging qualitative techniques, an interview study, case study and grounded theory. In-depth data collection and analysis can be completed to facilitate a broader data collection which will provide a representative sample and achieve saturation to ensure that adequate and quality data are collected to support the study. Quantitative analysis through statistical techniques (i.e. regression analysis) taking into account, the effectiveness of cybersecurity frameworks, and the effectiveness of decisions made by stakeholders on implementing cybersecurity measures.

Practical implications – This exploratory research demonstrates that organizations have actively implemented cybersecurity measure; however, there is a need to reduce the number and type of breaches, along with strengthening the cybersecurity framework to facilitate a preventative approach. In addition, factors that are used by an organization when investing in cybersecurity controls are heavily focused on

Compliance with ethical standards.

Availability of data and materials: This has been included with the manuscript as supplementary data.

Funding: This section is not applicable to this manuscript.

Disclosure of potential conflicts of interest: This section is not applicable to this manuscript.

Research involving human participants: Ethical approval: All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Helsinki declaration and its later amendments or comparable ethical standards.

Informed consent: Informed consent was obtained from all individual participants included in the study.

Transforming Government: People, Process and Policy
© Emerald Publishing Limited
1750-6166
DOI 10.1108/TG-11-2019-0112

compliance with government and industry regulations along with opportunity cost. Lastly, the decision-making process used when evaluating, implementing and investing in cybersecurity controls is weighted towards the technology organization and, therefore, may be biased based on competing priorities .

Social implications – The outcome of this study provides greater insight into how an organization makes decisions when implementing cybersecurity controls. This exploratory research shows that most organizations are diligently implementing security measures to effectively monitor and detect cyber security attacks. The pilot study revealed that the importance given to the decisions made by the CIO and Head of the Business Line have similar priorities with regard to funding the investment cost, implementing information security measures and reviewing the risk appetite statement. This parallel decision-making process may potentially have an adverse impact on the decision to fund cybersecurity measures, especially in circumstances where the viewpoints are vastly different .

Originality/value – Cybersecurity spend is discussed across the literature, and various approaches, methodologies and models are used. The aim of this paper is to explore the strategic decision-making approach that is used by organizations when evaluating and implementing cybersecurity measures. Using a survey study method, this paper explores the feasibility for development of a strategic decision-making framework that may be used when evaluating and implementing cybersecurity measures.

Keywords Cybersecurity, Economics in information security, Decision-making, Information security, Information risk management

Paper type Research paper

1. Introduction

This article explores the decision-making process of various stakeholders who are involved in the implementation of cybersecurity measures to safeguard sensitive data. Through use of a survey study, data was collected and used to understand the influence stakeholders have on an organization's decisions to fund cybersecurity measures.

Through this exploratory process, it is apparent that a wide range of principles are relevant to cybersecurity decision-making process. Specific security measures are important and should be implemented appropriately to alleviate cybersecurity threats. The outcomes of this exploratory research will provide the necessary data to determine if further research should be completed within the area of cybersecurity decision-making and its application to development of a strategic decision-making framework to broaden the current opportunity cost models.

2. Background

Economic optimization of information security is an area of interest to researchers and executives in most organizations. From a financial viewpoint, cost-benefit justification for security measures is impactful and necessary. Previous authors have focused on either the economics of information security or the decision-making process of information security investments.

This article aims to explore the viability for development of a strategic decision-making framework to assist organizations in effectively articulating the business impact of cybersecurity risks. This exploratory research will focus on three main areas to determine the appropriateness of the research for further in-depth analysis through a broader research approach:

- Why are current implementations of information security frameworks effective at identifying, monitoring and responding to information security threats?
- What factors are used by an organization when investing in cybersecurity controls?
- What decision-making mechanisms are organizations using when evaluating different security measures prior to implementation?

In reviewing previous literature on this topic, a list of questions was developed for use in analyzing journal articles and theses. The purpose of these questions is to provide a baseline of areas that the literature should address and to provide a focus for the exploratory research.

The basis of the literature review revealed two specific areas within the field of information security. The first area shows diverse defences against cyber security attacks using technical techniques, with the controls leveraged to include systems as well as policies and procedures. The second area focuses on the economics of information security, and many models and theories are used. Each area was reviewed in-depth to provide an understanding of its application to cybersecurity and the decision-making process used when evaluating and investing in various security measures.

2.1 Literature defining possible defences against cyber attacks

The literature defining possible defences against cyber attacks using technical techniques can be viewed from three general perspectives, specifically game theory, decision theory and expected utility theory. The primary focus in this area is on the use of technical techniques within various models.

Various methods are used in these studies that use technical techniques. The studies focus on the analysis of cyberattacks and their effects using game theory, security risk analysis models and event tree analysis as shown in these articles (Lee *et al.*, 2017; Feng and Wang, 2014; Orojloo and Azgomi, 2017; Henriques De Gusmão *et al.*, 2016; Fielder *et al.*, 2013; Zavgorodniy *et al.*, 2014).

These models are comprehensive, and some use both qualitative and quantitative methods and techniques to measure the security risk factors with causation using relevant systems. There are many limitations that result from the application of these methods to the proposed topic, specifically system complexities, type of organization, range of criteria and the utilization of a conceptual model to facilitate organizational decisions on information security spending.

In analyzing this area with the literature review, it is apparent that these models are well-defined and therefore would be out of scope for exploration within this research topic.

2.2 Literature defining economic models and theories on cybersecurity

The literature defining the economics of information security focuses on the strategic decisions made by organizations when implementing cybersecurity controls. Various models are used to determine ideal spending on information security measures. A traditional approach is shown in the study of Bojanc and Jerman-Blazic (2008), who propose a standard method for the assessment of the necessary ICT security countermeasures. The method classifies threats, assets and vulnerabilities of the ICT systems through a security risk analysis. Quantification of the ICT security investment is shown, making this method applicable to enterprise security risk scenarios.

In comparison Gordon and Loeb (2002), Gordon *et al.* (2016) "introduced an economic model to determine the optimal amount to invest in protecting a given set of information". In this study, the optimal amount to spend is viewed as a minimal fraction of the expected loss and uses a range of vulnerabilities in which investment is unwarranted. The study also shows that "an increase in vulnerability of an information set increases the optimal investment in information security". This economic model has become the industry framework and is leveraged by many researchers.

Researchers, Huang *et al.* (2008), developed a model for analyzing strategies for security investments under various assumptions. This framework leverages the Gordon and Loeb (2002)

model changing the risk assumption condition from a risk-neutral decision maker. This economic model examined the ideal security investment with the condition of a risk-averse decision maker. The study focuses on the literature to demonstrate that the decisions made in high performance organizations indicate risk aversion, as shown in Fiegenbaum and Thomas (1988) and Jegers (1991).

Organizations with risk-averse decision makers have a greater tendency to invest in security measures for risk reduction and encounter less capital constraint than organizations with performance that is below average.

Researchers leverage agency theory to demonstrate that a decision maker is risk-averse if their wealth portfolio is connected to the organization's performance (Wiseman and Gormez-Mejia, 1998).

Researchers conclude that risk-averse organizations will invest in security measures; therefore, a risk-aversion economic model for security investment would provide executive insight into how organizations should make decisions when investing in security measures.

Researchers (Mayadunne and Park, 2016), "attempt to determine how investment decisions change given information sets of varying breach probabilities and potential losses". The study takes into account previous models and approaches, specifically:

- the economic models of Gordon and Loeb (2002) and Huang *et al.* (2008);
- the expected utility theory of Von Neuman and Morgenster (2007); and
- an approach to understanding and influencing the decision of an attack (Cremonini and Nizovtsev, 2006).

Researchers model the cybersecurity investment behavior of a risk-taking decision maker in comparison to either a risk-neutral or risk-averse decision maker.

In addition to the models described above on information security spend using opportunity cost models, processes for decision-making relating to the purchase of security measures have been researched, as seen in Avgerou (2000). There are variations among industries, organizations, categories of individuals, technologies, organizational structure and risk profiles, resulting in varied outcomes of cybersecurity spending by executives. There is a distinction between the decision-making processes regarding the purchase of security measures and the purchase of information technology. They differ in the manner in which a decision is viewed by technical individuals in comparison to business employees. Therefore, the variance in viewpoint impacts the decision outcome, as shown by (Albrechtsen and Howden, 2009; Carty *et al.*, 2012; Johnson, 2009).

This article, through the use of a survey study will explore the area of information security decision making leveraging the research completed by Dor and Elovici (2016). Using grounded theory, researchers design a conceptual model that shows the current practices for decision-making about information security investment in organizations across industries. The framework takes into consideration that organizations may have different views, specifically depending on the stakeholder who finances the security measures, the organization's industry, structure and role of the Chief Information Security Officer's (CISO). The study reveals that leveraging a conceptual model can help relevant stakeholders during the decision-making process.

3. Cybersecurity spending

Cybersecurity spending is discussed across the literature, and various approaches, methodologies and models are used. The aim of this article is to explore the feasibility for

development of a strategic decision-making framework that may be used when evaluating and implementing cybersecurity measures.

3.1 Methodology used for evaluating cybersecurity spending

A pilot study was conducted to evaluate the ways in which decisions are made as it relates to cybersecurity spending. The purpose of the pilot study was to determine the feasibility for developing a strategic framework to minimize cybersecurity risks, with a focus on the decision-making process by applicable stakeholders within organizations. Through using three discussion questions as noted above, this pilot study explores the rationale for determining cybersecurity spend within organizations.

The pilot study research design used an inductive, qualitative approach and used a combination of techniques using a combined cross-sectional and time series horizon. The partnership research design applied a two-phased approach within the pilot study. To elaborate on partnership research designs, this approach "typically involves combining more than one method, such as a questionnaire survey and interviews, where both assume similar importance in the study [. . .]. When combined, the interview data will contain greater detail, clarifications and added explanations; the questionnaire data will contain shorter answers, possibly more focused, but will be able to cover responses from a wider range [. . .]" (Easterby-Smith *et al.*, 2015).

- Phase 1 – Interview study: The qualitative approach focused on seven participants who provided input to refine the survey study questionnaire.
- Phase 2 – Survey study: The qualitative approach focused on information gathered through an online descriptive survey study using a five-point Likert scale. The approach used in this qualitative research design included seven participants who provided input to refine the survey study questionnaire.

This approach ensured that the breadth of knowledge of the participants would be applied to the survey study, thus improving the clarity of information obtained when the survey was completed by the online participants. The interview method was chosen to facilitate the triangulation and complementarity of the participants' experiences in the strategic decision-making process for implementing cybersecurity controls. This approach was incorporated into the survey study to elaborate, corroborate and clarify the intent of the questions published in the online descriptive survey study, thus providing a greater level of confidence in the results.

This approach was used within the qualitative pilot study research design, as it allows for a systematic way to analyze the feedback and apply it to the survey study questionnaire. Using individual participants to review the survey questionnaire:

- facilitated a deeper understanding of the participants' perspectives on the intent of each survey question; and
- allowed for experienced industry individuals with direct knowledge of the topic and of pilot studies to provide input on the approach as well as the context of each question.

This approach facilitated redesigning survey questions to include:

- Likert scales;
- demographical questions;
- groupings of questions within categories;

- the ability to prioritize answers;
- the wording and applicability of each question;
- adding drop down/pick list options;
- reviewing the estimated time to complete;
- the number of questions on the questionnaire;
- asking the same type of question more than once throughout the survey; and
- the type of instrument used.

The output from these interviews was used in the following ways:

- to facilitate development of the descriptive online survey study questionnaire; and
- to supplement future work to be completed on this topic.

The design of the interview study within this pilot study facilitated flexibility; it allowed interaction between the researcher and participant, the completion of a combination of a semi-structured analysis of the investigated topic, the identification of common themes and the use of the information to further enhance the descriptive survey study questionnaire.

3.2 Survey study

The descriptive survey design was used because it provides a pre-specified data collection method to facilitate the collection of data on variables of interest with this pilot study. The survey made it possible to draw from a large, distributed population on a specific topic in the field of cybersecurity.

This survey design generated a description of the topic in terms of the distribution of the relevant variables and can play an exploratory role, in which certain statistical techniques (i.e. cluster analysis) can be used to identify underlining patterns. An online questionnaire was used as the primary data collection instrument, as it uses a standardized, structured set of questions to measure variables important within this area; these include the following:

- the effectiveness of current implementations of information security frameworks; and
- the decision-making process when evaluating, implementing and investing in information security controls.

The survey was published from September 5, 2018 to February 12, 2019 and had 324 views.

In total, 32% of the individuals who viewed the survey participated, for a total of 100 participants, with 88 completed and 12 partially completed surveys providing a representative sample size. The survey was administered with an introduction that provided obtained informed consent from the respondent.

The data from the survey responses were used to directly answer the discussion questions. Preliminary analysis focused on verification of the data prior to analysis, specifically:

- checking for errors;
- managing missing values;
- transforming the data to perform analysis; and
- checking scale reliability.

Descriptive statistics, such as the sample mean and standard deviation, were used to analyze, summarize and simplify the survey data.

3.3 Survey study results

The results from the survey were interesting and indicative of a survey that is replicable. The survey results were categorized into three classifications:

(1) the effectiveness of current implementations of cybersecurity frameworks;

(2) factors that are used by an organization when investing in cybersecurity controls; and

(3) the decision-making process used when evaluating, implementing and investing in cybersecurity controls.

The data received from the online survey study were used to answer the following discussion questions:

3.3.1 Why are current implementations of cybersecurity frameworks effective in identifying, monitoring and responding to cybersecurity threats? In analyzing the data, 93 respondents stated that they currently leverage government and industry frameworks when implementing cybersecurity measures. In addition, 84 respondents based their decision-making mechanisms on validating compliance with government regulations, industry standards and internal policy.

In total, 54% of respondents indicated that they had experienced a type of cybersecurity breach, prioritized as follows: malware/ransomware, phishing, lost/stolen computer media and external/data breach, where 94% of respondents expressed the average dollar loss as between $0-$1m.

Over 75% of respondents believe they can detect, respond to and monitor a security incident; however, they are not able to prevent a security incident from occurring within their environment. These respondents believe that their organization is in compliance with government and industry standards.

In total, 89 respondents indicated that their organization measures the effectiveness of the implemented cybersecurity framework according to the following priorities:

- compliance;
- audit/assurance testing;
- key performance indicators;
- capacity maturity models; and
- cost, taking into account that 50% of respondents indicated that their organization is a risk-averse environment.

3.3.2 What factors are used by an organization when investing in cybersecurity controls? In total, 87 respondents indicated that the decision-making mechanisms used by their organization when evaluating and implementing different security measures primarily focus on:

- compliance with government and industry regulations;
- investment cost;
- impact of either a breach or fine;
- either reputational or brand risk; and

- ease of use by the business.

3.3.3 What decision-making mechanisms are organizations using when evaluating different security measures prior to implementation? The results of the survey study provided a perspective on the importance of stakeholders making decisions on implementing cybersecurity measures within their organization. A total of 89 respondents indicated that the following hierarchy of decision makers:

- Chief Technology Officer (CTO);
- Chief Information Security Officer (CISO);
- Head of Business Line;
- Chief Information Officer (CIO), and
- Board of Directors.

Respondents believe that the CTO and CISO have the primary responsibility for funding the investment cost in their organization, and 66% of respondents indicated that their organization's investment budget is between $1 and $5m annually. Stakeholders are involved during the implementation of cybersecurity measures in the following ways, as prioritized by 89 respondents:

- directly involved in the decision-making mechanism;
- attend meetings on evaluating cybersecurity measures;
- involved in implementation activities related to cybersecurity measures; and
- supporting the cybersecurity function.

This exploratory research demonstrates that although organizations have actively implemented cybersecurity frameworks, there is a need to enhance the decision-making process to reduce the number and type of breaches, along with strengthening the cybersecurity framework to facilitate a preventative approach. In addition, factors that are used by an organization when investing in cybersecurity controls are heavily focused on compliance with government and industry regulations along with opportunity cost. Lastly, the decision-making process used when evaluating, implementing and investing in cybersecurity controls is weighted towards the technology organization and, therefore, may be biased based on competing priorities.

4. Discussion and conclusion

Most organizations are faced with an array of choices when deciding on funding as it relates to cybersecurity measures. Funding the investment cost to provide a secure environment can be complex. Cost-benefit analyses, risk appetite and business trade-offs are some of the areas that are factored into the overall decision-making process. The results of the survey study showed that the following areas are critical in an organization's decision-making process when allocating funds for cybersecurity measures:

- *Allocation of budget* – Although 74% of respondents believe that their organization has allocated a large enough budget to respond to or detect a cybersecurity breach, 93% of participants believe that their organization's cybersecurity budget is insufficient to ensure appropriate cybersecurity measures that would prevent a breach.

- *Ability to prevent a cybersecurity breach* – Although 74% of respondents believe that their organization can detect a cybersecurity breach in a timely manner, 81% of participants believe that their organization is unable to prevent a cybersecurity breach, with 11% indicating that their organization has encountered more than 15 breaches (Figure 1).

4.1 Measuring the effectiveness of implemented frameworks

In total, 91% of participants believe that their organization's current information security framework implementation is ineffective to prevent a cyber security breach.

A total of 89 respondents believe that their organization measures the effectiveness of the current information security framework implementation by: compliance with policy, audit and assurance testing, key performance indicators, cost and capacity maturity model.

4.1.1 Risk level. In total, 50% of the 88 respondents indicated that their organization's decision-making process is aligned with a risk-averse methodology, and as noted within most of the economic models presented earlier in this article, this would directly impact the cost-benefit analysis (Figure 2).

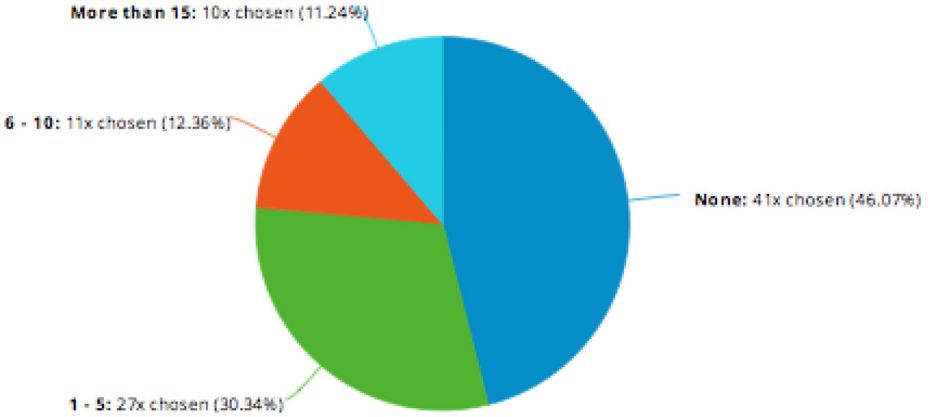


Figure 1.
Number of information security breaches that an organization has encountered

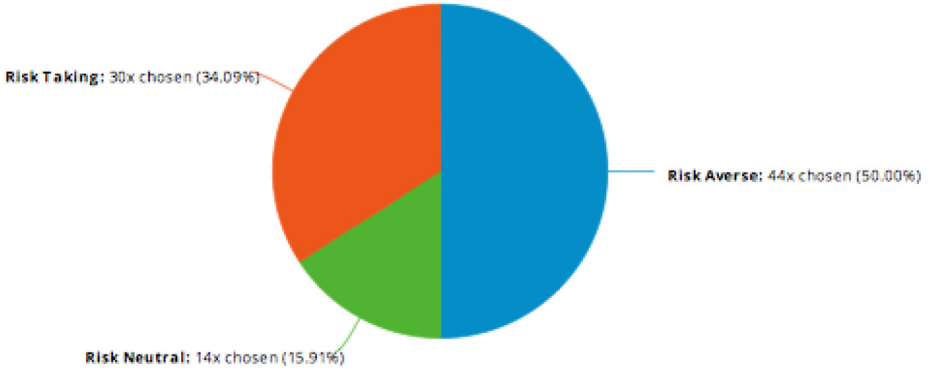


Figure 2.
Level of risk that an organization operates within

4.1.2 Importance of decision maker. The results of the survey study showed that the importance given to the decisions made by the CIO and Head of the Business Line have similar priorities with regard to:

- funding the investment cost;
- implementing information security measures; and
- reviewing the risk appetite statement.

This parallel decision-making process may potentially have an adverse impact on the decision to fund cybersecurity measures, especially in circumstances where the viewpoints are vastly different.

The literature review identified that there is limited research in the area of information security decision-making. One article was identified within this area, focusing on the research completed by Dor and Elovici (2016). It is apparent from the results of the survey study that the cybersecurity decision-making process takes into account an elaborate series of decisions that require input from many stakeholders within an organization. Using this type of decision-making process would require an understanding of key aspects within an organization's landscape, including a measure of the implementation of the cybersecurity framework, a funding model for cybersecurity measures, the risk appetite within an organization and the impact that a breach would have on an organization. Therefore, further work is required to understand and develop an appropriate decision-making framework to minimize cybersecurity risks. Developing this type of strategic framework would require a more in-depth research approach.

5. Implication for research, practice and/or society

The outcome of this exploratory research provides a relationship between theory and practice by demonstrating that most organizations are diligently implementing security measures to effectively monitor and detect cyber security attacks. The implications this pilot study has on practice is extensive, as it focuses on a broad range of areas to include risk, funding and type and impact of cyber security breaches encountered. The pilot study clearly demonstrated that 94% of participants believe their organization is in compliance with company policy and applicable regulations, and the organization can adequately detect, respond and monitor a security incident. In parallel, it was highlighted that ninety one per cent of respondents believe their organization is unable to prevent a security incident from occurring. This clearly identifies the need to further research this area.

The research can be used in practice to influence public policy, government regulations and industry standards. The pilot study revealed that the decision-making mechanism used by most organizations today requires further review to reduce the number of cyber security breaches through preventative measures. Specific security measures are important and should be proactively implemented appropriately to alleviate cybersecurity threats. The outcomes from this exploratory research provides a baseline to assist with further work on defining a strategic framework to minimize cybersecurity risks. This framework can be integrated with current industry frameworks to strengthen economic and commercial impact by contributing to the cyber security industry body of knowledge. The pilot study provided the relevant information required to demonstrate the feasibility for development of this type of framework, and it demonstrated an approach that is intended to be used within a larger-scale study to support this initiative.

6. Further work

There were several limitations of the pilot study, and these can be incorporated into the next phase of this research. Further development of the survey study instrument should be considered, possibly by leveraging a more robust tool such as Qualtrics and randomly allocating the positions of the questions to avoid order effects that may bias participants completing the survey. The partnership research design could be expanded to facilitate quantitative and qualitative techniques in parallel with equal weight, leveraging qualitative techniques such as an interview study, a case study and grounded theory. In-depth data collection and analysis can be completed to facilitate a broader collection of data, which will provide an appropriate representative sample and achieve saturation to ensure that adequate and quality data are collected to support the study. Quantitative analysis can be completed through statistical techniques (i.e. regression analysis) taking into account:

- the effectiveness of cybersecurity frameworks; and
- the effectiveness of decisions made by stakeholders on implementing cybersecurity measures.

References

Albrechtsen, E. and Howden, J. (2009), "The information security digital divide between information security managers and users", *Computers and Security*, Vol. 28 No. 6, pp. 476-490.

Avgerou, C. (2000), "Information systems: what sort of science is it?", *Omega (Omega)*, Vol. 28 No. 5, pp. 567-579.

Bojanc, R. and Jerman-Blazic, B. (2008), "An economic modelling approach to information security risk management", *International Journal of Information Management*, Vol. 28 No. 5, pp. 413-422.

Carty, M., Pimont, V. and and Schmid, D. (2012), "Measuring the value of information security investments", IT@Intel White Paper.

Cremonini, M. and Nizovtsev, D. (2006), "Understanding and influencing attackers' decisions: implications for security investment strategies", *Presented at the Workshop on the Economics of Information Security*, June 26-28, *Cambridge*.

Dor, D. and Elovici, Y. (2016), "A model of the information security investment decision-making process", *Computers and Security*, Vol. 63, pp. 1-13.

Easterby-Smith, M., Thorpe, R. and Jackson, P.R. (2015), *Management and Business Research*, Sage, London.

Feng, N., Wang, H.J. and Li, M. (2014), "A security risk analysis model for information systems causal relationships of risk factors and vulnerability propagation analysis", *Information Sciences*, Vol. 256, pp. 57-73.

Fiegenbaum, A. and Thomas, H. (1988), "Attitudes toward risk and the risk-return paradox: prospect theory explanations", *Academy of Management Journal*, Vol. 31 No. 1, pp. 85-106.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C. and Smeraldi, F. (2013), "Decision support approaches for cyber security investment", *Decision Support Systems*, Vol. 86, pp. 13-23.

Gordon, L.A. and Loeb, M.P. (2002), "The economics of information security investment", *ACM Transactions on Information and System Security (Tissec)*, Vol. 5 No. 4, pp. 438-457.

Gordon, L.A., Loeb, M.P. and Zhou, L. (2016), "Investing in cybersecurity: insights from the Gordon-Loeb model", *Journal of Information Security*, Vol. 7 No. 2, pp. 49-59.

Henriques De Gusmão, A.P., Camara e Silva, L., Maisa, M., Silva, A., Poleto, T. and Costa, A.P.C.S. (2016), "Information security risk analysis model using fuzzy decision theory", *International Journal of Information Management*, Vol. 43, pp. 25-34.

Huang, C.D., Hu, Q. and Behara, R.S. (2008), "An economic analysis of the optimal information security investment in the case of a risk-averse firm", *International Journal of Production Economics*, Vol. 114 No. 2, pp. 793-704.

Jegers, M. (1991), "Prospect theory and the risk-return relation: some Belgian evidence", *Academy of Management Journal*, Vol. 34 No. 1, pp. 215-225.

Johnson, A. (2009), "Business and security executives' view of information security investment drivers: results from a dephi study", *Journal of Information Privacy and Security*, Vol. 5 No. 1, pp. 3-27.

Lee, S., Kim, S., Choi, K. and Shon, T. (2017), "Game theory-based security vulnerability quantification for social internet of things", *Future Generation Computer Systems*, Vol. 82, pp. 1-9.

Mayadunne, S. and Park, S. (2016), "An economic model to evaluate information security investment of risk-taking small and medium enterprises", *International Journal of Production Economics*, Vol. 182, pp. 519-530.

Orojloo, H. and Azgomi, M.A. (2017), "A game-theoretic approach to model and quantify the security of cyber-physical systems", *Computers in Industry*, Vol. 88, pp. 44-57.

Von Neuman, J. and Morgenster, O. (2007), *Theory of Games and Economic Behaviour*, Princeton University Press, Princeton, NJ.

Wiseman, R.M. and Gormez-Mejia, L.R. (1998), "A behavioural agency model of managerial risk taking", *The Academy of Management Review*, Vol. 23 No. 1, pp. 133-153.

Zavgorodniy, V., Lukyanov, P. and Nazarov, S. (2014), "The selection algorithm of mechanisms for management of information risks", *Procedia Computer Science*, Vol. 31, pp. 440-448.

Further reading

Alali, M. Almogren, A. Hassan, M.M. Rassan, I.A.L. and Bhuiyan, M.Z.A. (2017), "Improving risk assessment model of cyber security using fuzzy logic inference system", Computer and Security.

Albrechtsen, E. and Howden, J. (2009), "The information security digital divide between information security managers and users", *Computers and Security*, Vol. 28 No. 6, pp. 476-90.

Alkaabi, A. (2014), "Strategic framework to minimize information security risks in the UAE", PhD, University of Bedfordshire.

Baranyi, J. and Buss DA Silva, N. (2017), "The use of predictive models to optimize risk of decisions", *International Journal of Food Microbiology*, Vol. 240, pp. 19-23.

BIN Ishaq Alseiari, K. (2015), "The management of risk awareness in relation to information technology (MERIT)", PhD, University of Gloucestershire.

Birks, M. and Mills, J. (2015), *Grounded Theory: A Practical Guide*, SAGE Publication, London.

Bojanc, R., Jerman-Blažič, B. and Tekavčič, M. (2012), "Managing the investment in information security technology by use of a quantitative modelling", *Information Processing and Management*, Vol. 48 No. 6, pp. 1031-1052.

Borgonovo, E., Cappelli, V., Maccheroni, F. and Marinacci, M. (2018), "Risk analysis and decision theory: a bridge", *European Journal of Operational Research*, Vol. 264 No. 1, pp. 280-293.

Campos, J., Sharma, P., Jantunen, E., Baglee, D., Fumagalli, L. and Slotwiner, D.J. (2016), "The challenges of cybersecurity frameworks to protect data required for the development of advanced maintenance", *Procedia Cirp*, Vol. 47, pp. 222-227.

Cavusoglu, H., Mishra, B. and Ragunathan, S. (2004), "A model for evaluating IT security investments", *Communications of the Acm*, Vol. 47 No. 7, pp. 87-92.

Cavusoglu, H., Raghunathan, S. and Raghunathan, W. (2008), "Decision-theoretic and game-theoretic approaches to IT security investment", *Journal of Management Information Systems*, Vol. 25 No. 2, pp. 281-304.

Cherdantseva, Y., Hilton, J., Rana, O. and Ivins, W. (2016), "A multifaceted evaluation of the reference model of information assurance and security", *Computers and Security*, Vol. 63, pp. 45-66.

Cho, S. (2003), "Risk analysis and management for information security", PhD, University of London, Royal Holloway.

Comes, T., Hiete, M., Wijngaards, N. and Schultmann, F. (2011), "Decision maps: a framework for multi criteria decision support under severe uncertainty", *Decision Support Systems*, Vol. 52 No. 1, pp. 108-118.

DE Bruijn, H. and Janssen, M. (2017), "Building cybersecurity awareness: the need for evidence-based framing strategies", *Government Information Quarterly*, Vol. 34 No. 1, pp. 1-7.

Dresner, D.G. (2011), "A study of standards and the mitigation of risk in information systems", PhD, University of Manchester.

Dutta, A. and Mccrohan, K. (2002), "Management's role in information security in a cyber economy", *California Management*, Vol. 45 No. 1, pp. 67-87.

Ericson, C.A.I. (2005), *Hazard Analysis Techniques for System Safety*, John Wiley and Sons.

Fazlida, M.R. and Said, J. (2015), "Information security: risk, governance and implementation setback", *Procedia Economics and Finance*, Vol. 28, pp. 243-248.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C. and Smeraldi, F. (2013), "Decision support approaches for cyber security investment", *Decision Support Systems*, Vol. 86, pp. 13-23.

Finne, T. (1998), "A conceptual framework for information security management", *Computers and Security*, Vol. 17 No. 4, pp. 303-307.

Gabriela Roldán-Molina, A.B., Almache-Cueva, M., Silva-Rabadão, C., Yevseyeva, I., Basto-Fernandes, V. and Yevseyeva, V.B.F. (2017), "A comparison of cybersecurity risk analysis tools. Centeris – International Conferences on Enterprise Information Systems Barcelona", *Procedia Computer Science*, Vol. 121, pp. 568-575.

Ge, X.Y., Yuan, Y.Q. and Lu, L.L. (2011), "An information security maturity evaluation mode", *Procedia Engineering*, Vol. 24, pp. 335-339.

Gordon, L.A., Loeb, M.P. and Lucyshyn, W. (2003), "Sharing information on computer systems security: an economic analysis", *Journal of Accounting and Public Policy*, Vol. 22 No. 6, pp. 461-485.

Gordon, L.A. and Loeb, M.P. (2006), *Managing Cyber-Security Resources: A Cost-Benefit Analysis*, McGraw-Hill.

Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2015), "The impact of information sharing on cybersecurity underinvestment: a real options perspective", *Journal of Accounting and Public Policy*, Vol. 34 No. 5, pp. 509-519.

Grunske, L. and Joyce, D. (2008), "Quantitative risk-based security prediction for component-based systems with explicitly modeled attack profiles", *Journal of Systems and Software*, Vol. 81 No. 8, pp. 1327-1345.

Huang, C.D. and Behara, R.S. (2013), "Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints", *International Journal of Production Economics*, Vol. 141 No. 1, pp. 255-268.

Johnson, A. (2009), "Business and security executives' view of information security investment drivers: results from a dephi study", *Journal of Information Privacy and Security*, Vol. 5 No. 1, pp. 3-27.

Joshi, C. and Singh, U.K. (2017), "Information security risks management framework: a step towards mitigating security risks in university network", *Journal of Information Security and Applications*, Vol. 35, pp. 128-137.

Jouini, M., Rabai, L.B.A. and Khedri, R. (2015), "A multidimensional approach towards a quantitative assessment of security threats", *Procedia Computer Science*, Vol. 52, pp. 507-514.

Kemkhadze, N. (2004), "Information and optimisation in investment and risk measurement", PhD, University of Warwick, Warwick Business School.

Kolkowska, E., Karlsson, F. and Hedström, K. (2017), "Towards analysing the rationale of information security non- compliance: devising a value-based compliance analysis method", *The Journal of Strategic Information Systems*, Vol. 26 No. 1, pp. 39-57.

Lavine, M.K. (2007), "Cyber security information sharing in the United States: an empirical study including risk management and control implications, 2000-2003", PhD, City University London.

Lee, Y.J., Kauffman, R.J. and Sougstad, R. (2011), "Profit maximizing firm investments in customer information security", *Decision Support Systems*, Vol. 51 No. 4, pp. 904-920.

Leuprecht, C., Skillicorn, D.B. and Tait, V.E. (2016), "Beyond the castle model of cyber-risk and cyber-security", *Government Information Quarterly*, Vol. 33 No. 2, pp. 250-257.

Mortazavi-Alavi, R. (2016), "A risk-driven investment model for analysing human factors in information security", PhD, University of East London.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. and Sadhukhan, S.K. (2013), "Cyber-risk decision models: to insure IT or not?", *Decision Support Systems*, Vol. 56, pp. 1-26.

Nazareth, D. and Choi, J. (2015), "A system dynamics model for information security management", *Information and Management*, Vol. 52 No. 1, pp. 123-134.

Ochoa, D.C.R., Correia, R., Peña, J.I. and Población, J. (2015), "Expropriation risk, investment decisions and economic sectors", *Economic Modelling*, Vol. 48, pp. 326-342.

Pettigrew, A. (2009), *The politics of organizational decision-making*, Routledge.

Posey, C., Roberts, T.L., Lowry, P.B. and Hightower, R.T. (2014), "Bridging the divide: a qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders", *Information and Management*, Vol. 51, pp. 551-567.

Purser, S.A. (2004), "Improving the ROI of the security management process", *Computers and Security*, Vol. 23 No. 7, pp. 542-546.

Rahimian, F., Bajaj, A. and Bradley, W. (2016), "Estimation of deficiency risk and prioritization of information security controls: a data-centric approach", *International Journal of Accounting Information Systems*, Vol. 20, pp. 38-64.

Rhee, H.-S., Ryu, Y.U. and Kim, C.-T. (2012), "Unrealistic optimism on information security management", *Computers and Security*, Vol. 31 No. 2, pp. 221-232.

Rodriguez, E. (2010), "Knowledge management applied to enterprise risk management", PhD, Aston University.

Rose, S., Spinks, N., Canhoto, A.I.2., Management Research, Applying The Principles. Abingdon, Oxon, Routledge. Ryan, J.J.C.H., Mazzuchi, T.A., Ryan, D.J., Lopez DE LA Cruz, J. and Cooke, R. (2012), "Quantifying information security risks using expert judgment elicitation", *Computers and Operations Research*, Vol. 39 No. 4, pp. 774-784.

Rue, R., Pfleeger, S. and Ortiz, D. (2007), "A framework for classifying and comparing models of cyber security investment to support policy and decision-making", *The sixth workshop on the economics of information security (WEIS07)*.

Saleh, M.S. and Alfantookh, A. (2015), "A new comprehensive framework for enterprise information security risk management", *Procedia Economics and Finance*, Vol. 28, pp. 243-248.

Shameli-Sendi, A., Aghababaei-Barzegar, R. and Cheriet, M. (2016), "Taxonomy of information security risk assessment (ISRA)", *Computers and Security*, Vol. 57, pp. 14-30.

Tsiakis, T. and Stephanides, G. (2005), "The economic approach of information security", *Computers and Security*, Vol. 24 No. 2, pp. 105-108.

VAN Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J. and Kusev, P. (2017), "Risk perceptions of cyber-security and precautionary behaviour", *Computers in Human Behaviour*, Vol. 75.

VAN Staalduinen, M.A., Khan, F., Gadag, V. and Reniers, G. (2017), "Functional quantitative security risk analysis (QSRA) to assist in protecting critical process infrastructure", *Reliability Engineering and System Safety*, Vol. 157, pp. 23-24.

VON Solms, R. and VAN Niekerk, J. (2008), "From information security to cyber security", *Computers and Security*, Vol. 38, pp. 97-102.

Webb, J., Ahmad, A., Maynard, S.B. and Shanks, G. (2014), "A situation awareness model for information security risk management", *Computers and Security*, Vol. 44, pp. 14-30.

Wiseman, R.M. and Gormez-Mejia, L.R. (1998), "A behavioural agency model of managerial risk taking", *The Academy of Management Review*, Vol. 23 No. 1, pp. 133-153.

Wu, Y., Feng, G., Wang, N. and Liang, H. (2015), "Game of information security investment: Impact of attack types and network vulnerability", *Expert Systems with Applications*, Vol. 42 Nos 15/16, pp. 6132-6146.

Yevseyeva, I., Morisset, C. and VAN Moorsel, A. (2016), "Modeling and analysis of influence power for information security decisions", *Performance Evaluation*, Vol. 98, pp. 36-51.

About the author

Tara Kissoon is a multi-certified Technology, Risk and Security Leader with 20 years of technology experience, 13 years of executive experience in the financial services industry. She brings continued success on leading Technology, I.T. Risk and Security programs within large organizations. She is acknowledged as a leader, security architect and trusted advisor with a talent for effective resource management, steering traditional and cross-functional staff to achieve short and long-term business objectives. Tara has a Masters of Science (MSc) in Information Security with Merit from Royal Holloway College, University of London and a Masters of Business Administration (MBA) with Distinction from Rotman School of Business, University of Toronto. She is a Certified Information Systems Auditor (CISA) and a Certified Information Systems Security Professional (CISSP). Tara Kissoon can be contacted at: tara@it-rs.org

For instructions on how to order reprints of this article, please visit our website:
www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: **permissions@emeraldinsight.com**