Investing in IT security: Managerial Insights on Resource Allocation – A Case Study

Yueran Zhuo, Mississippi State University, 324 McCool Hall, Mississippi State, MS 39759, Tel: 662.325.1998, Email: yzhuo@business.msstate.edu

Senay Solak, University of Massachusetts Amherst, 121 Presidents Drive, MA 01003, Tel: 413.545.5681, Email: solak@isenberg.umass.edu

Yi Zou, University of Massachusetts Amherst, 121 Presidents Drive, MA 01003, Tel: 413.545.5625, Email: yzou@isenberg.umass.edu

ABSTRACT

IT security is an inseparable operational component for any business that utilizes information systems. Given this significance, organizational decision makers are increasingly concerned about the economic aspects of IT security and seeking proper techniques for evaluating their investment decisions relating to IT security. While extant research has suggested numerous decision approaches to determining the optimal level of organizational IT security investments, most of them has not distinguished and taken into account the losses caused by different forms of security breaches and the benefits of deploying different types of IT security countermeasures. In this paper, we seek to fill in this important research gap by proposing a comprehensive framework of IT security investment management. Specifically, we utilize a two-stage stochastic programming model to delineate and examine the dynamic effects of a firm's security countermeasure portfolio mix. We validate the applicability of our model with a numerical case study on firms in public service sector. Our findings suggest that firms with different values of information assets should not only allocate different amounts of budgets for IT security, but also implement different allocation strategies for detecting and preventing IT security breaches.

Keywords: IT security investments, budget allocation optimization, IT security countermeasure portfolio, stochastic programming

1. INTRODUCTION

Information systems are an integral part of today’s business environment. According to a new report by Ponemon (2016), IT security attacks cost a typical large firm $7.7 million per year on average. Meanwhile, the global IT security investments have increased from $64 billion in 2011 to $120 billion by 2017 with an annual growth rate of more than 11% (Salgarkar 2013). As a result, firms are more concerned about the effectiveness of their investments in IT security, and whether their investment portfolio is aimed towards maximizing returns (Richardson 2010).

While extant research has proposed numerous decision approaches to determining the optimal level of organizational IT security investments (e.g., Cavusoglu et al., 2008; Herath & Herath, 2008; Li et al., 2021; Wang et al., 2008), neither the academic literature nor the existing industrial practice has been able to produce definitive guidelines on such issues. As compared to other types of IT investments, IT security investments pose unique challenges for organizational decision makers to assess and determine the investment effectiveness. In particular, IT security risks and vulnerabilities are not static, and they evolve with the strategic interactions between firms and hackers (Cavusoglu et al., 2008). The corresponding decision process involves a higher level of dynamics, where technological developments and increasing sophistication in threats to IT result in an ever-changing investment environment. As such, it is difficult for firms to estimate and measure returns from investing in IT security, and characterize the uncertainty around these returns.

In this paper, we first address the challenges pertaining to IT security investment management, and then develop a comprehensive framework for assessing the economic values of different categories of IT security countermeasures. Our research centers on 1) specifying the defining components in the investment environment for IT security, and 2) examining how a firm should determine the overall amount of IT security investment as well as the investment allocations over different security countermeasure categories. We utilize a two-stage stochastic programming model to reveal the dynamic effects of a firm’s security countermeasure portfolio mix, and validate the model applicability with a numerical case study. That is, we derive generic policies that would maximize expected returns from IT security investments and apply the analysis to a sample industry for managerial insights.

2. GENERAL FRAMEWORK

We start the construction of our framework (Figure 1) by identifying the key components that define the investment environment for IT security. These include attacks that target a firm’s information assets, countermeasures that a firm can deploy against such attacks, and the potential total losses that the firm can incur due to a breach of its information assets.

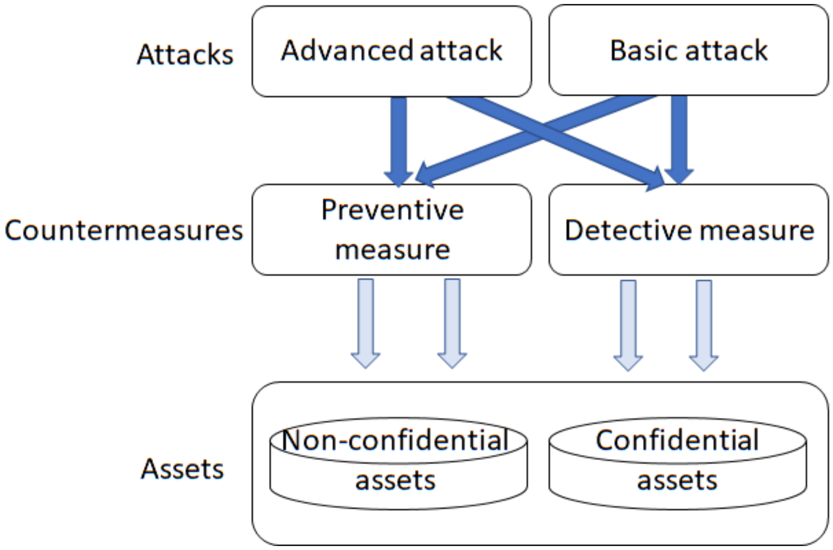


Figure 1. Cross-relationships between the potential losses of a firm, attacks that can result in these losses, and countermeasures that can be deployed against the attacks.

2.1. Components of the Framework

Attacks. We follow a structure proposed by Richardson (2010) to consider two types of attacks: basic attacks and advanced attacks. Basic attacks are typically simple and opportunistic attacks that are pervasively spread to the public to exploit vulnerabilities in information systems. Advanced attacks are usually the most sophisticated attacks and are generally customized for an individual organization.

Countermeasures. We follow the classification by Stoneburner et al. (2002) to distinguish different types of IT security countermeasures into two major categories: preventive and detective countermeasures. Preventive countermeasures include methods such as biometrics and access control are aimed at preparing the firm against attacks before any breach can take place. Detective countermeasures are aimed at identifying and removing an attack during or after the occurrence of a breach.

Potential Losses. A firm's potential losses refer to the value of systems and information the firm possesses which are at risk of an IT security attack. We adopt the categorization by Herson et al. (2003) which suggest that the assets to be identified as being either confidentiality related, or integrity/availability (non-confidential) related. The three components of IT security are connected by multidimensional cross-relationships as illustrated in Figure 1. As shown, losses can be caused by both basic and advanced attacks, while both preventive and detective countermeasures can be deployed against the types of attacks. Hence, a firm's IT security investment strategy should depend on the distribution of the potential losses over the basic and advanced attacks.

2.2. The Decision Process of IT Security Investment

Investment in IT security is an iterative multi-step procedure involving the three components introduced above. In Figure 2, we provide a visual representation of the typical steps involved in this dynamic process.

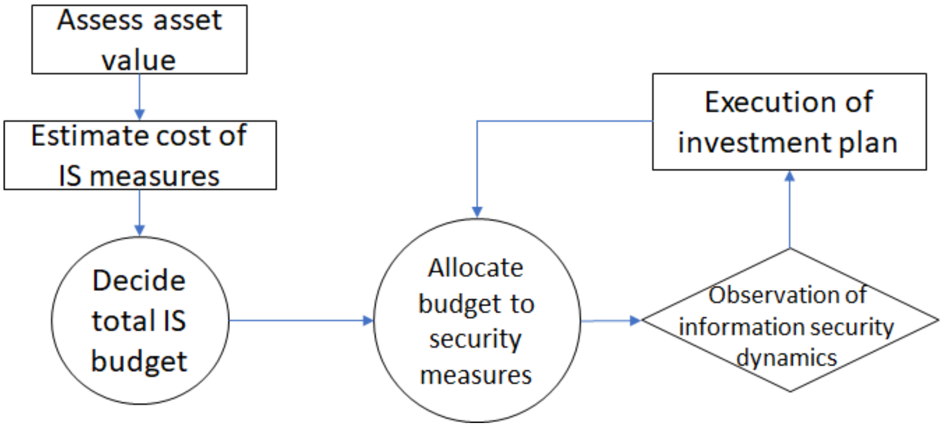

Assess asset value
Estimate cost of IS measures
Decide total IS budget
Allocate budget to security measures
Observation of information security dynamics
Execution of investment plan

Figure 2. Representation of the dynamic decision process for IT security investments of a firm.

The process starts with the firm assessing the value of its information assets, which corresponds to the maximum possible losses that the firm can incur due to a breach of its information systems. The next step is the estimation of the expected costs for perfect protection. The third step answers the key question as how much the firm should invest in IT security.

In step four, the firm considers all relevant factors and decides on the allocation of the budget over the IT security countermeasures for potential investment. The firm continuously observes the IT security dynamics and learns about the effectiveness of the implemented countermeasures. The investment portfolio is then updated as necessary at specific intervals. Our analysis in this paper captures the dynamic process and aims to provide insights for the two key IT security investment decisions highlighted above.

3. STOCHASTIC MODELING OF IT SECURITY INVESTMENTS

3.1. Functional Representation of Countermeasure Effectiveness

We assume that a firm maintains a set $S = \{s_1, s_2\}$ of types of potential losses, where s_1 corresponds to confidentiality-related losses, while s_2 refers to integrity/availability-related losses. These losses can result from a set $A = \{a_1, a_2\}$ of attacks with a_1 and a_2 referring to basic and advanced attacks, respectively. The expected loss las of type $s \in S$ due to an attack $a \in A$ represents the value to be protected and is typically expressed in dollars. In response to the potential attacks on its information systems, the firm deploys a set $O = \{o_1, o_2\}$ of countermeasures, consisting of detective and preventive security measures denoted respectively as o_1 and o_2. Each countermeasure type $o \in O$ has an estimated level of effectiveness $e_{oa}(x_o)$ on attack type $a \in A$, which is a function of the amount x_o invested in countermeasure type o. The effectiveness function $e_{oa}(x_o)$ is defined separately for each attack and countermeasure pair, and refers to the percent reduction of losses on any information asset due to attack type *a* achieved by utilizing countermeasure type o. For example, $e_{o_1 a_1}(x_{o_1}) = 0.8$ would imply that an 80% reduction in potential losses can be achieved against basic attacks by investing xo1 dollars in detective countermeasures.

We consider the effectiveness function $e_{oa}(x_o)$ must satisfy the following conditions as also noted by Gordon and Loeb (2002): $e_{oa}(0) = 0$; $e_{oa}(x_o) \to \beta_{oa}$ when $x_o \to \infty$; $\frac{\partial e_{oa}(x_o)}{\partial x_o} > 0$ and $\frac{\partial^2 e_{oa}(x_o)}{\partial x_o^2} < 0$ for all $o \in O$ and $a \in A$.

Therefore, we define the following function to model the effectiveness rate of a countermeasure category against a given type of attack on information systems:

$$e_{oa}(x_o) = \beta_{oa} - e^{-(\alpha_o x_o - \ln \beta_{oa})} = \beta_{oa} - \beta_{oa} e^{-\alpha_o x_o} \qquad \forall o \in O, a \in A \qquad (1)$$

Then, we further consider the joint effectiveness of IT security countermeasures. One can view the joint effectiveness of two countermeasures as a virtual countermeasure added to the system. To capture this, we define the interdependency coefficient $\rho_{oo'}$ for two countermeasure categories $o, o' \in O$, and use it to represent the loss under joint effectiveness between the two countermeasures as $f_a l_{as} \sqrt{1 - e_{oo'a}(x_o, x_{o'})}$, where $e_{o'oa}(x_o, x_{o'}) \in [0,1]$ and is defined as:

$$e_{oo'a}(x_o, x_{o'}) = \rho_{oo'} e_{oa}(x_o) + \rho_{oo'} e_{o'a}(x_{o'}) - \rho_{oo'}^2 e_{oa}(x_o) e_{o'a}(x_{o'}) \quad \forall o \in O, a \in A \qquad (2)$$

3.2. Modeling the Dynamics of Countermeasure Effectiveness

IT security countermeasures are designed to follow a life cycle resulting in variation in effectiveness β_{oa} over time *t*, specifically as $\beta_{oa}(t)$. To capture these dynamics of information life-cycle curve, or whether it will become obsolete at a faster or slower rate. We note that the exact information on the shape of this curve is not known to the firm due to the uncertainties associated with technological performance. As a IT security product is used and its performance over time is observed, the firm will gain knowledge about where the product might be on its life cycle. Then, the firm may readjust budget allocations over different countermeasures.

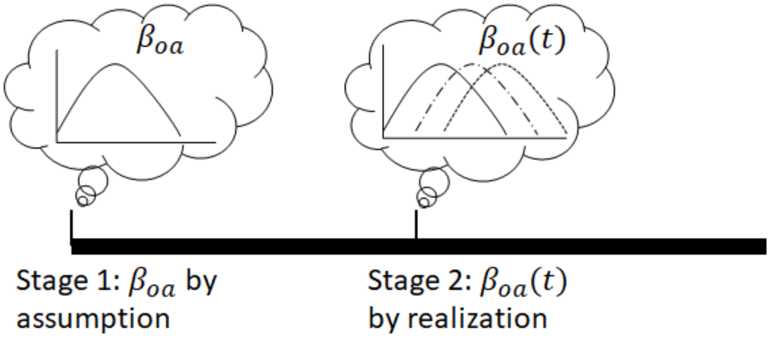

β_{oa}
$\beta_{oa}(t)$
Stage 1: β_{oa} by assumption
Stage 2: $\beta_{oa}(t)$ by realization

Figure 3. Representation of the two-stage decision process for IT security investments of a firm.

The above effects can be captured through a two-stage process as depicted in Figure 3. An estimate for the parameter $\beta_{oa}(t)$ is assumed to be revealed in the second stage for future periods, and the revised decisions are based on these revelations.

3.4. Two-stage Stochastic Programming Model with Endogenous Uncertainty

The decision framework above can be modeled through a stochastic programming approach with endogenous uncertainty. We assume that a certain level of investment is necessary for information gathering on the performance of the IT security countermeasures.

We refer to this sufficient level of investment for a countermeasure category o as θ_o. If the initial investment in a countermeasure is less than the threshold θ_o, then no information will be gained, and the later period investments will be made based on the life cycle structure initially assumed. The firm will then make second stage investment with inaccurate information.

Given these definitions, a stochastic programming formulation for the IT security investment problem can be expressed as follows:

$$\min_{\mathbf{x},\mathbf{e},\mathbf{b}\in R^+} \sum_{\omega\in\Omega} p^{\omega}\left[\sum_{k\in K}\sum_{s\in S}\sum_{a\in A}\sum_{t\in T} f_{at} l_{ast}\left(\prod_{o,o'\in O}\sqrt{1-e^{k\omega}_{oo'at}\left(x^{k\omega}_{o},x^{k\omega}_{o'}\right)}\right)+\sum_{k\in K}\sum_{o\in O} x^{k\omega}_{o}\right]$$

$$\text{s.t.}\quad e^{k\omega}_{oo'at}\left(x^{k\omega}_{o},x^{k\omega}_{o'}\right)=\rho_{oo'}e^{k\omega}_{oat}\left(x^{k\omega}_{o}\right)+\rho_{oo'}e^{k\omega}_{o'at}\left(x^{k\omega}_{o'}\right)-\rho^{2}_{oo'}e^{k\omega}_{oat}\left(x^{k\omega}_{o}\right)e^{k\omega}_{o'at}\left(x^{k\omega}_{o'}\right) \qquad (3)$$

$$\forall o,o'\in O, a\in A, t\in T, k\in K, \omega\in\Omega \qquad (4)$$

$$e^{1\omega}_{oat}\left(x^{1\omega}_{o}\right)=\beta_{oat}-\beta_{oat}e^{-\alpha^{1}_{o}x^{1\omega}_{o}} \qquad \forall o\in O,\ a\in A, t\in T^{1}, \omega\in\Omega \qquad (5)$$

$$e^{2\omega}_{oat}\left(x^{2\omega}_{o}\right)=b_{oat}-b_{oat}e^{-\alpha^{2}_{o}x^{2\omega}_{o}} \qquad \forall o\in O,\ a\in A, t\in T^{2}, \omega\in\Omega \qquad (6)$$

$$b_{oat}=\beta_{oat}(1-\sigma_{o})+\beta_{oat\omega}\sigma_{o} \qquad \forall o\in O,\ a\in A, t\in T^{2}, \omega\in\Omega \qquad (7)$$

$$e^{k\omega}_{oat}\left(x^{k\omega}_{o}\right)\geq \underline{e^{k}_{oa}},\ x^{k\omega}_{o}\geq \underline{x^{k}_{o}} \qquad \forall o\in O, \omega\in\Omega \qquad (8)$$

$$x^{1\omega}_{o}\leq\theta_{o}+M\sigma_{o}, x^{1\omega}_{o} \qquad \forall o\in O, \omega\in\Omega \qquad (9)$$

$$\sum_{k\in K}\sum_{o\in O} x^{k\omega}_{o}\leq B \qquad \forall\omega\in\Omega \qquad (10)$$

$$x^{1\omega}_{o}=x^{1\omega'}_{o} \qquad \forall o\in O, \omega, \omega'\in\Omega \qquad (11)$$

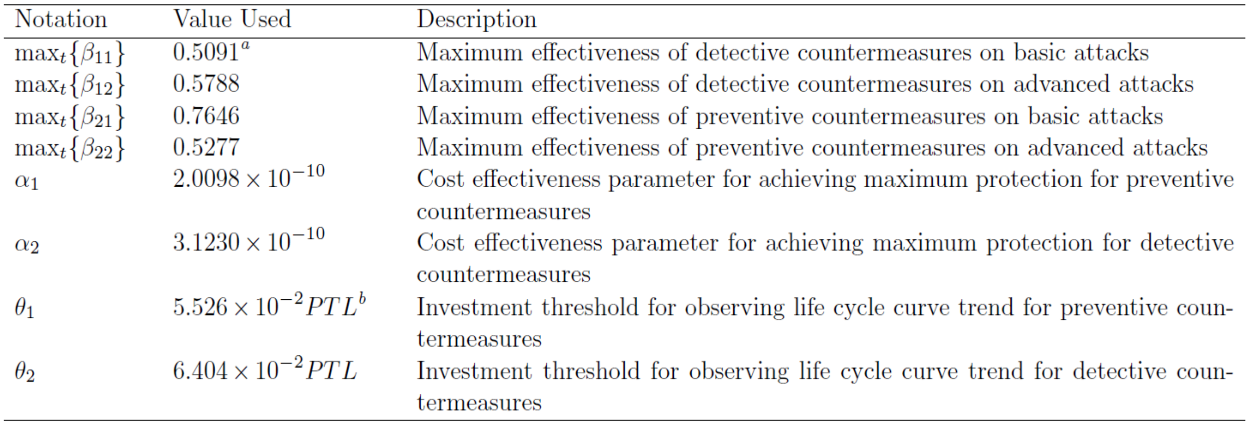
In this model, the objective function (3) involves the minimization of the sum of the investment costs and expected losses of the firm over the planning horizon. This represents the expected total expenditure or total cost under IT security investment. Constraints (4) through (6) define the effectiveness of countermeasures in both joint and individual forms. Note that the maximum achievable effectiveness level $\beta_{oat\omega}$ in (6) is replaced by its second stage counterpart, which is a variable defined by equation (7). This relationship stipulates to be realized as the scenario-dependent value $\beta_{oat\omega}$ only if $\sigma_o = 1$ i.e. if investment in a countermeasure category is greater than the corresponding threshold. Otherwise, no information is revealed so that β_{oat} will still be used in the second stage. Constraints (8) reflect the minimum protection requirements imposed by external factors in terms of countermeasure effectiveness and investment levels in both the first and second stages. Constraints (9), where M denotes a tight bound as in typical big-M formulations, define the binary variable σ_o . Constraints (10) state the investment budget limitation over the entire planning horizon, while constraints (11) are the nonanticipativity constraints that ensure that first stage decisions are the same for all scenarios.

4. POLICY ANALYSIS BASED ON A CASE STUDY

4.1. Data Preparation for the Case Study

In this section, we conduct a case study on the public service industry to illustrate some policy insights of IT security investment management. This case study is inspired by data collected from 8 IT security management/executive practitioners and 6 IT security technician/engineers. The summary of the survey results is presented as parameter estimates in Table 1. The parameter on the synergetic effects of IT security countermeasures takes value as $\rho_{12} = \rho_{21} = 0.32$.

Table 1. Description of data used to represent parameters of the decision framework based on survey



Notation	Value Used	Description
$\max_t\{\beta_{11}\}$	0.5091^a	Maximum effectiveness of detective countermeasures on basic attacks
$\max_t\{\beta_{12}\}$	0.5788	Maximum effectiveness of detective countermeasures on advanced attacks
$\max_t\{\beta_{21}\}$	0.7646	Maximum effectiveness of preventive countermeasures on basic attacks
$\max_t\{\beta_{22}\}$	0.5277	Maximum effectiveness of preventive countermeasures on advanced attacks
α_1	2.0098×10^{-10}	Cost effectiveness parameter for achieving maximum protection for preventive countermeasures
α_2	3.1230×10^{-10}	Cost effectiveness parameter for achieving maximum protection for detective countermeasures
θ_1	$5.526 \times 10^{-2} PTL^b$	Investment threshold for observing life cycle curve trend for preventive countermeasures
θ_2	$6.404 \times 10^{-2} PTL$	Investment threshold for observing life cycle curve trend for detective countermeasures

The countermeasure effectiveness life cycle curves are created from the technical support of commercial detective and preventive countermeasure applications from McAfee (2013) and Symantec (2014). The public service industry has a cyber environment profile with basic attack vs. advanced attack frequencies being 63 vs. 37.

4.2. Analysis I: Optimal Investment in IT security

In our analysis, the optimal investment level is represented as a percentage of the total value of the information assets that the firm holds. In Figure 4, we demonstrate our finding for the public service industries. The horizontal axis in the plot is investment in IT security, and the vertical axis shows the value of expected total costs after investments. The figure shows a leveling point when increasing the investment will no longer yield a decrease in expected total costs. In other words, any investment beyond that level is not cost-effective. We refer to the budget size at this leveling point as the optimal level of investment in IT security.

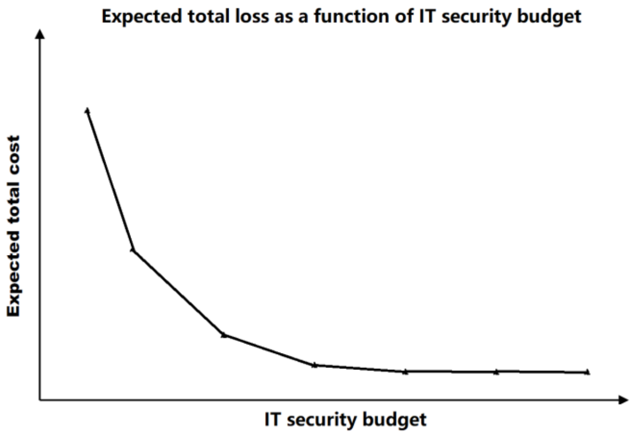


Figure 4. Change in expected costs as a function of IT security budget for the public sector.

4.3. Analysis II: Optimal Allocation of the IT security Budget over Countermeasure Categories

In this section, we investigate optimal budget allocation policies for IT security investments in public service industry. The question is: what should be the optimal allocation of budget over detective and preventive countermeasures for different industries?

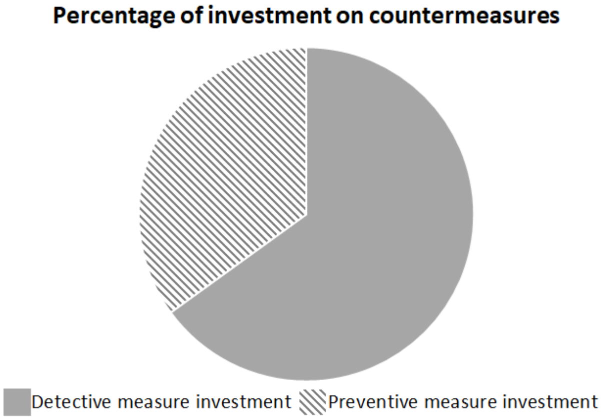


Figure 5. Budget allocation over IT security countermeasure categories for public sector.

The Figure 5 shows the percentage of investment on detective countermeasures in the initial investment period for public service industry. The reason for the consideration of the initial period investment here is that the decision maker can always resolve the model based on a rolling horizon and apply the results from the first stage decisions. The public service industry should invest about twice more in detective technologies than preventive ones, corresponding to an approximate split of 65% versus 35%. We note that this ratio will vary for different industries with different cyber-attack environments.

5. CONCLUSIONS AND FUTURE RESEARCH

The severity of attacks targeting business information systems and the challenges in dealing with them are significant concerns not only in the U.S. but also all over the globe. As a result, it is critical for chief information officers and other IT practitioners to take informed approaches to determining the overall amount of IT security investment as well as the specific investment allocations over different countermeasure categories.

This paper addresses these challenges and develops a comprehensive framework involving significant components in IT security investment management. A stochastic optimization model is then built upon this framework that adopts high-level categorizations and captures a generic view of the decision-making process with learning effects. A numerical case study indicates an optimal investment budget for IT security. Our research work suggests that each industry should have a unique spending structure regarding detective and preventive countermeasures. For the public service industry, this ratio should be an approximate split of 65% versus 35%.

As the future steps for this study, we will expand the data-driven analysis to cover more industries featuring different basic attack versus advanced attack frequency ratios. To do this, we will evaluate the optimal IT security investment decisions over a spectrum of basic versus advanced attack frequency ratios and fit the individual industries into several categories on this spectrum. We will rely on published information sources such as Ponemon (2016) for the data on such ratios for the industries.

We will also explore the risk aspect of IT security investment, which is defined by the variation of returns over different realizations of uncertainty in the IT security investment context. To do so, we plan to adopt a conditional value at-risk measure and incorporate it into the IT security investment optimization problem. We will then study how the risk attitude of the firms affects their optimal decisions on IT security investment through the integrated model.

In summary, our study provides a general framework that addresses a critical practical issue in IT security investment. The model can be adopted by any firm that wants to apply the model by fitting it with the precise information of their IT security practice. Our study also added to the research stream where quantitative methods can be adopted to evaluate the effectiveness of IT security investment with uncertainty, which opens doors for many potential follow-up studies on similar topics.

REFERENCES

Cavusoglu, H., Raghunathan, S., & Yue, W. T. (2008). Decision-theoretic and game-theoretic approaches to IT security investment. *Journal of Management Information Systems, 25*(2), 281-304.

Herath, H. S., & Herath, T. C. (2008). Investments in information security: A real options perspective with Bayesian postaudit. *Journal of Management Information Systems, 25*(3), 337-375.

Herson, D., P. Davis, Y. Klein, U. Essen, H. Tabuchi. 2003. Generally accepted IT security principles. Tech. rep., National Institute of Standards and Technology, Reston, VA.

Li, H., Yoo, S., & Kettinger, W. J. (2021). The roles of IT strategies and security investments in reducing organizational security breaches. *Journal of Management Information Systems*, *38*(1), 222-245.

McAfee. 2013. McAfee product&technology support lifecycle. http://www.mcafee.com/us/support/ support-eol-software-utilities.aspx#swu_ebus_server. Retrieved January 6, 2013.

Ponemon, L. 2016. 2016 cost of cyber crime study & the risk of business innovation. Tech. rep., Ponemon Institute, Traverse City, MI

Richardson, R. 2010. CSI computer crime and security survey. Tech. rep., Computer Security Institute, New York City, NY.

Salgarkar, R. 2013. Cyber security market expected to reach $120.1 billion and grow at a CAGR of 11.3% by 2017. http://www.sbwire.com/press-releases/ cyber-security-market-expected-to-reach-1201-billion-grow-at-a-cagr-of-113-by-2017-373420. htm. Retrieved January 10, 2013

Stoneburner, G., A. Goguen, A. Feringa. 2002. Risk management guide for information technology systems. Tech. rep., National Institute of Standards and Technology, Reston, VA.

Symantec. 2014. Symantec corporation enterprise support.http://www.symantec.com/business/support/ index?page=releasedetails&key=54619. Retrieved December 18, 2012.

Wang, J., Chaudhury, A., & Rao, H. R. (2008). Research note—A value-at-risk approach to information security investment. Information Systems Research, 19(1), 106-120.