Measuring and Optimizing Cybersecurity Investments: A Quantitative Portfolio Approach

Abstract ID: I636

Abstract

Cybersecurity is an inseparable component of business operations in any industry that utilizes information systems. Hence, the problem of cybersecurity investment, defined by the cost-effectiveness of investing on cybersecurity countermeasures, is an important financial and operational decision for most businesses. We propose a modeling framework that incorporates major components relevant to cybersecurity practice, and study the characteristics of optimal cybersecurity investment decisions for a firm. The uncertainty in the problem is captured through a stochastic programming framework. A case study based on real cybersecurity practice of an organization is also presented, where the results cast managerial insights for cybersecurity investment that can be widely applicable in typical businesses.

Keywords
cybersecurity investment, budget allocation, portfolio approach, stochastic programming

1. Introduction

Information systems are an integral part of today’s business environment. Businesses, government organizations, and the society rely on these systems for various transactions, most of which have huge financial implications. As a result, cyber attacks, i.e. attacks that breach information systems causing interruption of operations, loss of data and customer confidence, constitute a significant threat for firms. Cyber attacks have been increasing in frequency and sophistication over time, and defending the assets of a firm in response to these attacks have become a key operational issue. According to [15], a typical large firm with around 500 to 1000 employees experiences around 100 successful attacks per week, with an annual cost ranging from $1.4 million to $46 million. In 2012, U.S. government alone reported 1.8 billion attack incidents [10]. Based on an estimate by [1], the global cost of cyber crime on the world economy has reached $1 trillion per year.

The losses due to cyber attacks can be mitigated through investments in cybersecurity technologies and services. [7] and [9] define cybersecurity as an integral element in the management of a firm, and highlights its importance as a key area for the successful operation of a business. Given this significance, most firms typically utilize independent cybersecurity budgets, dedicated for investment towards protecting the assets of the firm against cyber attacks. While the type of the business plays a role in determining the ratio of the cybersecurity budget with respect to a firm’s overall information technology budget, it is well known that this ratio has been steadily increasing over the recent years, along with the actual dollar value allocated to cybersecurity [14]. As cybersecurity budgets increase along with available cybersecurity investment options, firms are more concerned about the effectiveness of their investments in cybersecurity measures, and whether their investment portfolio is aimed towards maximizing returns [16]. This is a challenging process due to several factors, which involve the difficulty of measuring returns from cybersecurity investments, as well as the difficulty of defining the uncertainty around these returns. Moreover, the corresponding decision process is a dynamic one, where technological developments and increasing sophistication in cyber attacks result in an ever-changing investment environment. In this paper, we address this dynamic decision problem, and develop a high level framework aimed at providing guidance to firms when allocating their cybersecurity budgets into different types of investment options. The framework utilizes potential loss information specific to a firm, as well as general information on the characteristics of different types of attacks and cybersecurity investments. Several analyses are then performed to identify policies that would maximize expected returns from the investments.

2. The General Cybersecurity Investment Framework

The core principle of cybersecurity consists of protecting three aspects of information: confidentiality, integrity and availability. For any given firm, this can be achieved by a set of systematic measures requiring active investment through allocation of firm’s resources. In this section, we present a generic framework that defines such cybersecurity
investment decisions, and how an optimization model can be built upon them. This decision framework is based on a comprehensive analysis of the available literature in the area and surveys with industry collaborators. We start the construction of our generic framework by identifying the key components of the cybersecurity investment problem, namely the assets that a firm holds, cyber attacks that target these assets, and countermeasures that a firm can deploy to protect its assets against these attacks.

A firm’s assets refer to the collection of systems and information that the firm possesses for the operation of the business. The preservation of the confidentiality, integrity and availability of these systems is the ultimate goal of cybersecurity. These three aspects and their interrelations help define a categorization of the assets into two main categories. Noting the distinction of confidentiality among the three aspects, [8] suggests that a firm’s assets can be grouped broadly as being either confidential assets or non-confidential assets. Confidential assets correspond to information that should not be disclosed to any third parties. For example, these can include customer personal data, intellectual properties, and other restricted files. Non-confidential assets any other assets that have value. In our paper we adopt this categorization in determining cybersecurity investment policies for different types of firms.

Cyber attacks correspond to all types of threats to the information systems of a firm, and represent the second key component that needs to be considered in a cybersecurity investment framework. A commonly adopted classification of cyber attacks is a three-shell structure proposed by [16], with the inner shell representing basic attacks, the middle shell representing malware attacks and outer shell representing more sophisticated or advanced attacks. Basic attacks are typically unsophisticated and opportunistic attacks, that are pervasively spread to the public in order to exploit any existing weaknesses in information systems. Malware attacks, on the other hand, are an extended version of the basic attacks, which has some level of customization based on the industry targeted. Advanced attacks are usually customized for an individual organization in a more deliberate way, and are more difficult to defend against due to their level of sophistication. [16] notes that most malware attacks would also fall in the category of advanced attacks as well. Hence, in our analysis, we include malware attacks as part of the advanced attacks, and use two main categorizations of cyber attacks, namely the basic and advanced attacks. It is worth noting that despite their relatively simplistic structure, basic attacks are not necessarily less harmful than advanced attacks, as they can occur very frequently and should be defended against on a daily basis [16].

Cybersecurity countermeasures are the set of security measures aimed at protecting the assets of a firm against cyber attacks. Although the term ‘countermeasure’ can typically refer to cybersecurity technology products, they can also include ‘soft’ security measures such as establishing security policies and training employees - as long as these measures serve to mitigate the losses due to cyber attacks. Based on the protection mechanisms used, [17] classify the types of countermeasures that a firm can deploy into two major categories: preventive countermeasures and detective countermeasures. The former includes methods such as encryption, use of forensic tools, and access control lists, and are aimed at preparing the firm against cyber attacks before any breach can take place. On the other hand, detective countermeasures are aimed at identifying and removing an attack during or after the occurrence of a breach. Such measures include tools such as anti-virus software, firewalls, and intrusion detection systems. Note that the soft measures mentioned above can be classified into either countermeasure category, depending on the nature of the measure.

The connection between the three major components of a cybersecurity investment framework, namely the assets, attacks, and countermeasures, is multidimensional with cross-relationships. More specifically, the two major categories of assets can be targeted by both basic and advanced attacks, while at the same time both preventive and detective countermeasures can be deployed against the two categories of attacks. Hence, a firm’s cybersecurity investment strategy, i.e. how much to invest in each type of countermeasure, should depend on the distribution of the potential losses over the basic and advanced attacks, as well as the effectiveness of each type of countermeasure on these attack categories. Clearly, these distributions vary for different types of firms. In parts of our analyses, we consider several representative industries, and identify optimal policies for typical firms in these industries.

Investment in cybersecurity is a dynamic process, where the three components introduced above are taken into account through an iterative multi-step procedure. The process starts with the firm assessing the value of its assets, which corresponds to the maximum possible expected loss that the firm can suffer due to cybersecurity breaches under different attack types. Note that the total maximum loss amount corresponds to an upper bound for the returns from cybersecurity investments. Taking into account this value at stake, and considering the fiscal situation of the company, the firm decides on a cybersecurity budget. The next steps involve the identification of investment options and their effectiveness in protecting the firm’s assets, and allocation of the budget over the set of countermeasures identified for potential investment. The step involving budget allocation to different cybersecurity investment options is critical with significant financial implications, and is the focus of this paper. We utilize stochastic modeling and develop policy
insights that can be used by firms when determining investment decisions on different types of countermeasures. Note that while a customized large-scale optimization model can be solved for a given instance of the problem that may be applicable to only a specific company, our goal is to derive generic insights that would apply to most businesses in certain major industries. Hence, rather than considering specific individual countermeasures or investment options, we use the general categories described above in defining all problem parameters, which allows for the derivation of generalizable and practically relevant insights for firms. After the identification and implementation of an investment portfolio, the firm continuously observes the cybersecurity dynamics, which involves learning about the effectiveness of the implemented countermeasures, and updates the investment portfolio as necessary at specific intervals. Our analysis in this paper captures some of these dynamics by modeling learning effects and portfolio adjustment options.

3. A Stochastic Model for Cybersecurity Investment Planning

In this section we introduce the general mathematical setup for the cybersecurity investment problem, which is further expanded through the characterizations of uncertain parameters and the development of a stochastic optimization model. We assume that a firm maintains a set $S = \{s_1, s_2\}$ of asset categories, where $s_1$ corresponds to confidential assets, while $s_2$ refers to non-confidential assets as described above. Note that the framework and the definition of the set $S$ are general, as other categorizations with additional asset types can also be used. On the other hand, we use the two-asset category classification of [8] in order to derive insights that are practically relevant and also clear to understand. The assets of the firm are subject to a set $A = \{a_1, a_2\}$ of cybersecurity attacks with $a_1$ and $a_2$ referring to basic and advanced types of attacks, respectively. The estimated maximum possible loss due to an attack $a \in A$ on asset $s \in S$ is denoted by $l_{sa}$, which represents the value to be protected and is typically expressed in dollars. This value can be estimated by considering all possible expenditures that would result due to the consequences caused by an attack. Such expenses typically consist of staff time, compensation and other services provided to customers.

In response to the potential cybersecurity attacks, the firm deploys a set $O = \{o_1, o_2\}$ of countermeasures, consisting of preventive and detective security measures, denoted respectively as $o_1$ and $o_2$. Each countermeasure type $o \in O$ has an estimated rate 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 $e_{oa}(x_o)$ refers to the ability of a countermeasure to reduce asset losses caused by a cyber attack, and is defined separately for each attack and countermeasure type. The quantitative loss that while a theoretical upper bound for $e_{oa}(x_o)$ can be solved for a given instance of the problem that may be applicable to only a specific company, our goal is to derive generic insights that would apply to most businesses in certain major industries. Hence, rather than considering specific individual countermeasures or investment options, we use the general categories described above in defining all problem parameters, which allows for the derivation of generalizable and practically relevant insights for firms. After the identification and implementation of an investment portfolio, the firm continuously observes the cybersecurity dynamics, which involves learning about the effectiveness of the implemented countermeasures, and updates the investment portfolio as necessary at specific intervals. Our analysis in this paper captures some of these dynamics by modeling learning effects and portfolio adjustment options.

3. A Stochastic Model for Cybersecurity Investment Planning

In this section we introduce the general mathematical setup for the cybersecurity investment problem, which is further expanded through the characterizations of uncertain parameters and the development of a stochastic optimization model. We assume that a firm maintains a set $S = \{s_1, s_2\}$ of asset categories, where $s_1$ corresponds to confidential assets, while $s_2$ refers to non-confidential assets as described above. Note that the framework and the definition of the set $S$ are general, as other categorizations with additional asset types can also be used. On the other hand, we use the two-asset category classification of [8] in order to derive insights that are practically relevant and also clear to understand. The assets of the firm are subject to a set $A = \{a_1, a_2\}$ of cybersecurity attacks with $a_1$ and $a_2$ referring to basic and advanced types of attacks, respectively. The estimated maximum possible loss due to an attack $a \in A$ on asset $s \in S$ is denoted by $l_{sa}$, which represents the value to be protected and is typically expressed in dollars. This value can be estimated by considering all possible expenditures that would result due to the consequences caused by an attack. Such expenses typically consist of staff time, compensation and other services provided to customers.

In response to the potential cybersecurity attacks, the firm deploys a set $O = \{o_1, o_2\}$ of countermeasures, consisting of preventive and detective security measures, denoted respectively as $o_1$ and $o_2$. Each countermeasure type $o \in O$ has an estimated rate 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 $e_{oa}(x_o)$ refers to the ability of a countermeasure to reduce asset losses caused by a cyber attack, and is defined separately for each attack and countermeasure type. The quantitative measure of $e_{oa}(x_o)$ is based on the historical trend of losses on any asset due to attack type $a$ achieved by utilizing countermeasure type $o$. For example, $e_{o_1a}(x_{o_1}) = 0.8$ would imply that an 80% reduction in potential losses can be achieved against basic cybersecurity attacks by investing $x_{o_1}$ dollars in preventive countermeasures. An important input is the definition of the effectiveness functions $e_{oa}(x_o)$ for each countermeasure and attack type. First, it is important to note that that while a theoretical upper bound for $e_{oa}(x_o)$ would be 1, such an effectiveness level is practically not achievable. Hence, we let $\beta_{oa} \leq 1$ denote the maximum attainable effectiveness by countermeasure type $o \in O$ against attack type $a \in A$. Given this, the effectiveness function $e_{oa}(x_o)$ must satisfy the following conditions, as also noted by [9]:

\[ e_{oa}(0) = 0; e_{oa}(x_o) \to \beta_{oa} \text{ when } x_o \to \infty; \frac{\partial e_{oa}(x_o)}{\partial x_o} > 0; \text{ and } \lim_{x_o \to \infty} \frac{\partial^2 e_{oa}(x_o)}{\partial x_o^2} > 0 \text{ for all } o \in O \text{ and } a \in A. \]

These properties imply that the function $e_{oa}(x_o)$ has to be concave and monotonically increasing on $x_o \in [0, +\infty)$, while asymptotically achieving the highest effectiveness level $\beta_{oa}$. Based on these conclusions, we define the following function to model the effectiveness rate of a countermeasure category against a given attack type:

\[ e_{oa}(x_o) = \beta_{oa} - e^{-(\alpha_o x_o - \ln \beta_{oa})}, \quad \forall o \in O, a \in A \]  

(1)

where $\alpha_o$ is a parameter determining the rate that the effectiveness curve reaches the maximum achievable level $\beta_{oa}$ as a function of the investment level $x_o$.

The effectiveness function for a countermeasure category $o$ on attack type $a$ corresponds to a relative measure defining the percent decrease in potential losses due to the utilization of countermeasures in category $o$. On the other hand, the return from an investment in a countermeasure needs to be defined in absolute terms in dollars based on the expected losses after the countermeasure implementation [9]. Given $l_{sa}$, namely the expected maximum possible loss due to attack type $a$ on asset $s$, realized losses under a single countermeasure protection is defined as $l_{sa} f_a (1 - e_{oa}(x_o))$, where $f_a$ represents the frequency of attack type $a$, based on the estimated number of such attacks during the planning period. The loss reduction here is a result of reduced number of successful attacks, and this leads to a multiplicative form for the total overall losses, expressed as $\sum_a \sum_s f_a l_{sa} (1 - e_{oa}(x_o))$. We can illustrate this structure by conceiving the countermeasures as layers of fences through which the attack infiltrates but gets weakened in terms of expected quantity layer after layer. Assuming the countermeasures to be working in an independent way, the attack confronted by the next layer is always what is left after the screening by the previous layer. Thus, the contribution of the next layer can be added through multiplication of its effectiveness by what is left.
Our model also captures interdependencies, as an important issue in estimating the value of cybersecurity investments is the synergy or redundancy effects between different countermeasure types. Continuing the layer example, we can view the dependencies of two countermeasures as virtual layers besides the real individual countermeasure layers. In other words, joint effectiveness of two countermeasure categories against an attack is not necessarily the product of their individual effectiveness rates. To capture such dependencies between two countermeasure categories \( o, o' \in O \), we define the interdependency coefficients \( \rho_{oo'} \), which is used to represent the loss under joint effectiveness between the two countermeasures as \( f_{oo'}(1 - \sum_{o' \in O} f_{o'o'}(x_o, x_{o'})) \), in which \( f_{oo'}(x_o, x_{o'}) \) is defined as:

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

such that the joint effectiveness has a nice implicit multiplicative form as follows.

\[
1 - e_{oo'}(x_o, x_{o'}) = (1 - \rho_{oo'}e_{oo}(x_o))(1 - \rho_{oo'}e_{o'o'}(x_{o'})) \quad \forall o, o' \in O, a \in A
\]

Note that such a structure enables a compact expression of the overall loss function. Defining \( \rho_{oo'} = 1 \), the term \( \sqrt{1 - e_{oo'}(x_o, x_{o'})} \) reduces to \( 1 - e_{oo}(x_o) \) when \( o = o' \). Hence, in order to express the total losses after cybersecurity investments by taking into account the joint effectiveness rates, we modify the basic total loss expression above as:

\[
L(x) = \sum_{t \in T} \sum_{a \in A} f_{oo'}(1 - \prod_{o, o' \in O} \sqrt{1 - e_{oo'}(x_o, x_{o'})})
\]

where \( x \) represents the vector defining the countermeasure investments in different countermeasure categories.

### 3.1 Modeling the Dynamics of Countermeasure Effectiveness

The cyber environment has an ever-changing nature, inevitably bringing in uncertainty to the cybersecurity investment planning process. The most significant uncertainty involves the effectiveness of countermeasures, both due to the dynamic nature of attacks and the probabilistic evolution of success in defending a firm’s assets against these attacks. Cyber attacks evolve rapidly over time in terms of strength and pattern, while some epochal events may trigger significant rise in cyber attacks that cause problems in certain industries. To this end, we introduce the time dimension into the attack frequency as \( f_a(t) \) which allows for non-homogeneity in attack frequencies over time without loss of any generality. In response, countermeasures are also designed to be updated frequently in order to catch up with the evolution of the attacks and maintain a certain effectiveness level. This can only be done over a specific period, resulting in a life-cycle type variation in a countermeasure’s maximum attainable effectiveness, i.e. \( \beta_{oo}(t) \), over time. This requires the definition of this parameter as a function of time \( t \), specifically as \( \beta_{oo}(t) \). However, the exact nature of this life-cycle is not known to a firm, which can only be estimated probabilistically for use as part of the cybersecurity investment planning process. Our modeling captures this dynamic uncertainty in effectiveness, as well as any learning effects that can take place over time.

As noted above, cybersecurity countermeasures, specifically those in the form of hardware and software, typically have effectiveness levels that vary depending on where the product is in its life cycle. The widely applied notion of product life-cycle is first introduced by [4], where an S-shaped life-cycle curve is partitioned into five phases: innovators, early adopters, early maturity, late maturity and laggard. Noting that cybersecurity products are typically well tested after development and become obsolete at the end of a period, we follow [11] and consider a three phase life-cycle for the effectiveness of cybersecurity countermeasures. These phases correspond to early adopters, early maturity, and late maturity. In the early adopter phase, the countermeasure is first introduced to the market, then at the early maturity phase the product gets gradually accepted and improved through market experience, and lastly, at the late maturity phase, the countermeasure is eventually replaced by competing products, resulting its obsolescence. More relevant, however, the shape of the effectiveness life-cycle curve differs based on the type of countermeasure. We specifically consider the differences between the two major countermeasure categories previously identified, namely the preventive countermeasures and detective countermeasures. [13] suggest that detective countermeasures typically have a sharp drop in their effectiveness towards the end of the product’s life-cycle. This is because such products are dependent on continuous updates by vendors, e.g. anti-virus and firewall applications relying on signature information about the latest virus database, so that the infiltrated attacks can be found in a timely manner. Thus, the effectiveness of these countermeasures drop at a higher rate once such updates stop. Preventive countermeasures, on the other hand, are more robust in the late maturity phase as the effectiveness relies primarily on the product design itself, as opposed to being dependent on continuous updates, such as in the cases of encryption algorithms and access control techniques. Considering these characteristics, as well as product life-cycle information available at [12], it is possible to plot general representative maximum effectiveness life-cycle curves for the two categories of countermeasures.
(a) Effectiveness life-cycle curves for the two major categories of cybersecurity countermeasures.  
(b) Demonstration of different realizations of $\beta_{oa}(t)$ in the second period, after initial investment and learning in the first period.  

Figure 1: Illustration of effectiveness life-cycle curves.

3.2 Modeling the Uncertainty in Countermeasure Effectiveness

While the maximum attainable effectiveness of a countermeasure will typically follow a life-cycle curve, a firm will not have exact information on the shape of this curve or as to where a specific product is placed on that curve at the time of acquisition and implementation. However, as a product is put to use and its performance over time is observed, the firm will gain knowledge about this information, specifically as to where the product might be on its life-cycle curve. This new information can be used to readjust budget allocations to different countermeasure types. The above effects can be captured through a two-stage process, where the firm makes an initial investment over a set of countermeasure categories, and then can readjust these investments based on endogenous information about the performance of the measures invested on. In this process, the parameter $\beta_{oa}(t)$ is assumed to be revealed in the second stage, and the revised decisions are based on these realizations.

We further describe this process through an example shown in Figure 1b. As depicted in the figure, it is assumed that the countermeasure effectiveness curve follows the segments of an early maturity phase in the first stage. The three possible realizations at the second stage can be either a backward shift $B$ towards less maturity, a no shift case $M$, or a forward shift towards more maturity $F$. The backward and forward shifts correspond to a life-cycle curve that respectively indicates less and more maturity at the start of the implementations, implying that the firm’s initial assumptions on the structure of the life-cycle curve was not accurate. In this two-stage stochastic set up, all combinations of life-cycle curve realizations correspond to a scenario. On the other hand, two countermeasure types are not necessarily equally sensitive towards different attacks, resulting in the diversification of the effectiveness life-cycle curve. In other words, the effectiveness life-cycle curves are considered not for each countermeasure, but for each countermeasure-attack pair separately.

3.3 Two-stage Stochastic Programming Model with Endogenous Uncertainty

The decision framework described above can be modeled through a stochastic programming approach involving endogenous uncertainty, where the latter is due to the dependence between the investment decisions made and the realized learning effects on the performance of different countermeasures.

In order to describe the dynamics involving changes of the input parameters $\beta_{oa}(t)$ over time, we discretize the planning horizon and represent such dynamics by using discrete time intervals. We let $t = 1, 2, \ldots, T$ refer to each of these intervals, and append the definition of the maximum effectiveness level and the attack frequency through the addition of a time subscript as $\beta_{out}$ and $f_{at}$, respectively. An important issue is the length of the period that a countermeasure stays in use before a new investment decision is made. This typically coincides with budget planning that might take place every year with periodical decisions in each quarter. In our implementations we assume that the second stage decisions take place 3 months after the initial investments on a portfolio of countermeasures and the whole planning horizon lasts for one year. On the other hand, to keep a generalized formulation, we assume that the second stage decision occurs after time period $T'$, which implies that periods $1, 2, \ldots, T'$ correspond to first stage periods, while the second stage periods are $T' + 1, T' + 2, \ldots, T$. We refer to the set of time periods in each stage as $T_1$ and $T_2$.

As described in Section 3.2, the uncertainty structure in the model involves a set of scenarios, each of which corresponds to a possible combination of life-cycle curve realizations, i.e. $\beta_{out}$ for $t = T' + 1, T' + 2, \ldots, T$, for a given countermeasure-attack category pair. The number of scenarios is dependent on the number of countermeasure and attack categories, as well as the the number of realization levels for each life-cycle curve. We denote a given scenario by $\omega \in \Omega$, where $\Omega$ is the set of all scenarios. Moreover, the notation for the uncertain parameter $\beta_{out}$ is appended with
A scenario index as $\beta_{out}$. Similarly, all second stage variables in the problem definition need to be defined through a scenario index, as they correspond to decisions that will be implemented after the realization of the scenario outcome. These definitions are further described later in this section.

A characteristic of our framework is that we capture the learning effects on the effectiveness of countermeasures that are implemented after the initial investment period. These learning effects are dependent on the amount of investment made into a countermeasure category. In other words, enough sampling needs to occur to reach a conclusion as to where a certain category of countermeasures is on the corresponding life-cycle, and this can only be achieved by making sufficient investment in that category. We refer to this sufficient level of investment for a countermeasure category $o$ as $\theta_o$. If the initial investment in a countermeasure category is less than the threshold $\theta_o$, then no information will be gained and the second stage investments will be made based on the life-cycle structure initially assumed, although in reality the effectiveness of the countermeasure category may be different than these assumed levels. Given that the realization of new information is dependent on the investment decisions made, this implies a setting with endogenous uncertainty. To model this structure in our formulation, we define the binary variable $\sigma_o$ for each $o \in O$, where it takes on a value of 1 if $x_o^1 \geq \theta_o$, and 0 otherwise. Note that we define the investment decisions separately for the first and second stages as $x_o^1$ and $x_o^{2\omega}$, respectively, where the latter variable is defined for each scenario as these decisions are made after scenario realizations.

In addition to these issues, the cybersecurity investment process takes place under certain constraints. The first deals with the budget constraint such that the total investment over the planning period can not be larger than a total available budget $B$. Moreover, the actual investment plan is always influenced by external factors, such as minimum protection requirements imposed by laws or regulations. Reflected in our model, these factors can be formulated as bounds on investment levels or countermeasure effectiveness levels. We define the parameters $\xi_o$ and $\xi_{out}$ to represent lower bounds on the investments and effectiveness rates for each countermeasure $o \in O$ against attack $a \in A$.

Given these definitions, a stochastic programming formulation for the cybersecurity investment problem we study in this paper can be expressed as follows:

$$
\begin{align*}
\min_{x \in R^+, \sigma \in \{0, 1\}} & \sum_{a \in A} \sum_{t \in T} \sum_{o \in O} f_{out}(a^t) \left( \prod_{o', \theta \in O} \sqrt{1 - e_{out}(x_{o'}^1, e_{o'}^1)} \right) + \sum_{o \in O} x_o^1 \\
& + \sum_{o \in O} b_o \left[ \sum_{a \in A} \sum_{t \in T} \sum_{o \in O} f_{out}(a^t) \left( \prod_{o', \theta \in O} \sqrt{1 - e_{out}(x_{o'}^{2\omega}, e_{o'}^{2\omega})} \right) + \sum_{o \in O} x_o^{2\omega} \right] \\
\text{s.t.} & \quad e_{out}(x_{o}^1, e_{o}^1) = p_{out} e_{out}(x_{o}^1) + p_{out} e_{out}(x_{o}^1) - p_{out} e_{out}(x_{o}^1) e_{out}(x_{o}^1) \\
& \quad \forall o, o' \in A, a \in A, t \in T^1 \\
& \quad e_{out}(x_{o}^{2\omega}, e_{o}^{2\omega}) = p_{out} e_{out}(x_{o}^{2\omega}) + p_{out} e_{out}(x_{o}^{2\omega}) - p_{out} e_{out}(x_{o}^{2\omega}) e_{out}(x_{o}^{2\omega}) \\
& \quad \forall o, o' \in A, a \in A, t \in T^2, \omega \in \Omega \\
& \quad e_{out}(x_{o}^1) = \beta_{out} - e^{-\alpha_{o}^1 t_{out}} - \ln\beta_{out} \\
& \quad \forall o, a \in A, t \in T^1 (7) \\
& \quad e_{out}(x_{o}^{2\omega}) = h_{out} - e^{-\alpha_{o}^{2\omega} t_{out}} - \ln h_{out} \\
& \quad \forall o, a \in A, t \in T^2, \omega \in \Omega (8) \\
& \quad b_{out} = \beta_{out} (1 - \sigma_o) + \beta_{out} \sigma_o \\
& \quad \forall o, a \in A, t \in T^2, \omega \in \Omega (9) \\
& \quad x_o^1, x_o^{2\omega} \geq 0, \quad \forall o \in O, \omega \in \Omega \\
& \quad e_{out}(x_{o}^1) \geq \xi_{out} \\
& \quad \forall o, a \in A, t \in T^1, t' \in T^2, \omega \in \Omega (11) \\
& \quad \sum_{o \in O} x_o^1 + x_o^{2\omega} \leq B \\
& \quad \forall o \in O, \omega \in \Omega (12) \\
& \quad x_o^1 \leq \theta_o + M \sigma_o \\
& \quad x_o^1 \geq \theta_o + M \sigma_o - 1 \\
& \quad \forall o \in O (13)
\end{align*}
$$

In this stochastic programming model, the objective is the minimization of the sum of the investment costs and expected total losses over the planning horizon. The objective function (4) represents the expected total expenditure under cybersecurity investment. The first two parts correspond to the first stage total loss under the utilization of countermeasures and the cost of such utilization, respectively. The last part is the expectation of the same expenditures under all the stochastic scenarios. In this objective function, the risk attitude of the decision maker is assumed to be risk neutral. Constraints (5) and (7) define the effectiveness of countermeasures in both joint and individual forms. Constraints (6) and (8) are the second stage versions of constraints (5) and (7) defined for each scenario. Note that the maximum achievable effectiveness level $\beta_{out}$ in constraint (5) is replaced by a second stage variable $b_{out}^{2\omega}$, which is
defined by (9). This relationship stipulates \( b_{out} \) to be realized as the scenario-dependent value \( \beta_{out,o} \) only if \( \sigma_o \geq \theta_o \), i.e. if investment in a countermeasure category is greater than the corresponding threshold. Otherwise, no information is revealed so that \( \beta_{out} \) will still be used in the second stage. Constraints (10) and (11) reflect the minimum protection requirements imposed by external factors in terms of investment and countermeasure effectiveness levels in both the first and second stages. Constraint (12) states the investment budget limitation over the entire planning horizon. Furthermore, constraints (13) define the binary variable \( \sigma_o \) which is used in the previous constraint (9). Our proposed model is a mixed integer nonlinear model with a non-convex feasible set and objective function. In the next subsection we demonstrate the procedures we use to transform this model into a linear mixed integer programming model for improved tractability.

### 3.4 Linearization of the Nonlinear Stochastic Programming Formulation

In the above formulation, constraints (3)-(9) and the objective function (4) involves nonlinearities, which we linearize through a systematic procedure. Here we start with the first stage constraints (5), (7) and the first term of the objective function (4) which do not involve stochastic parameters. To this end, we define two variables as \( I_{oat}(x_{o}^1) = \ln(1 - \beta_{oat} e_{oat}(x_{o}^1)) \) and \( E_{oat}(x_{o}^1, x_{o'}^1) = \ln(1 - e_{oat}(x_{o}^1, x_{o'}^1)) \). Employing the implicit multiplicative form of (5) introduced in section 3, \( E_{oat} \) and \( I_{oat} \) would have a linear relationship such that

\[
E_{oat}(x_{o}^1, x_{o'}^1) = I_{oat}(x_{o}^1) + E_{oat}(x_{o'}^1) \quad \forall o,o' \in O, a \in A, j \in T^1
\]

(14)

Because the problem is a minimization problem, \( I_{oat}(x_{o}^1) \) can be approximated by a series of K constraints:

\[
I_{oat}(x_{o}^1) \geq \bigoplus_{o,o' \in O} I_{oat}(x_{o}^1) + E_{oat}(x_{o'}^1) \quad \forall o,o' \in O, a \in A, j \in T^1, k = 1,..,K
\]

(15)

where \( u \) and \( v \) respectively represent the slopes and intercepts for the piecewise linear constraints. As the next step, we transform the nonlinear term in the first component of the objective function into:

\[
D_{at}(x_{o}^1, x_{o'}^1) = \ln \prod_{o,o' \in O} \sqrt{1 - E_{oat}(x_{o}^1, x_{o'}^1)} \quad \forall o,o' \in O, a \in A, j \in T^1
\]

(16)

It follows that \( D_{at}(x_{o}^1, x_{o'}^1) \) can be expressed as a function of \( E_{oat}(x_{o}^1, x_{o'}^1) \) as:

\[
D_{at}(x_{o}^1, x_{o'}^1) = \frac{1}{2} \sum_{o,o' \in O} E_{oat}(x_{o}^1, x_{o'}^1) \quad \forall a \in A, j \in T^1
\]

(17)

In order to be plugged back into the objective, we need to take the exponential of the transformed term \( D_{oat}(x_{o}^1, x_{o'}^1) \).

In the interest of conciseness of the expression, the term \( \prod_{o,o' \in O} \sqrt{1 - e_{oat}(x_{o}^1, x_{o'}^1)} \) is substituted by a single notation \( y_{at}(x_{o}^1, x_{o'}^1) \). Because exponential function is convex, (16) can as well be approximated by a series of K constraints:

\[
y_{at}(x_{o}^1, x_{o'}^1) \geq h_{at,k} + D_{at}(x_{o}^1, x_{o'}^1) + g_{at,k} \quad \forall a \in A, j \in T^1, k = 1,..,K
\]

(18)

with \( h \) and \( g \) referring to the slope and intercept for the linear approximation functions. For the linearization procedure of the second stage counterparts, notations \( I_{oat}(x_{o}^2), E_{oat}(x_{o}^2, x_{o'}^2), D_{at}(x_{o}^2, x_{o'}^2) \) and \( y_{at}(x_{o}^2, x_{o'}^2) \) are defined similarly and the following constraints are constructed:

\[
I_{oat}(x_{o}^2) \geq \bigoplus_{o,o' \in O} I_{oat}(x_{o}^2) + E_{oat}(x_{o'}^2) \quad \forall o,o' \in O, a \in A, j \in T^2, k = 1,..,K
\]

(19)

\[
E_{oat}(x_{o}^2, x_{o'}^2) = I_{oat}(x_{o}^2) + I_{oat}(x_{o'}^2) \quad \forall o,o' \in O, a \in A, j \in T^2, k = 1,..,K
\]

(20)

\[
D_{at}(x_{o}^2, x_{o'}^2) = \frac{1}{2} \sum_{o,o' \in O} E_{oat}(x_{o}^2, x_{o'}^2) \quad \forall a \in A, j \in T^2, k = 1,..,K
\]

(21)

\[
y_{at}(x_{o}^2, x_{o'}^2) \geq h_{at,k} D_{at}(x_{o}^2, x_{o'}^2) + g_{at,k} \quad \forall a \in A, j \in T^2, k = 1,..,K
\]

(22)

However, a challenge is brought by the constraints (8) and (9) that \( b_{oat} \) appears in the exponent with the involvement of binary variable \( \sigma_o \). Therefore the piecewise linear approximation of constraint (8) is achieved by the design of two sets of switching constraints using \( \sigma_o \) itself:

\[
I_{oat}(x_{o}^2) \geq \bigoplus_{o,o' \in O} I_{oat}(x_{o}^2) + E_{oat}(x_{o'}^2) - M \sigma_o \quad \forall o,o' \in O, a \in A, j \in T^2, k = 1,..,K
\]

(23)

\[
I_{oat}(x_{o}^2) \geq \bigoplus_{o,o' \in O} I_{oat}(x_{o}^2) + E_{oat}(x_{o'}^2) - M(1 - \sigma_o) \quad \forall o,o' \in O, a \in A, j \in T^2, k = 1,..,K
\]

(24)

where \( M \) denotes a tight bound as in typical big-M formulations. When the first stage investment reaches the threshold so that \( \sigma_o = 1 \), the second set of constraints will be applicable while the first set becomes redundant, and vice versa. Thus, the linearized formulation for the cybersecurity investment optimization problem can be expressed as:

\[
\min_{x \in \mathbb{R}^d, \sigma \in \{0,1\}} \sum_{s,S \in A} \sum_{a \in A} \sum_{t \in T^2} f_{at} I_{oat}(x_{o}^1, x_{o'}^1) + \sum_{o \in O} x_{o}^1 + \sum_{o \in O} p_{o} \left[ \sum_{s,S \in A} \sum_{a \in A} \sum_{t \in T^2} f_{at} I_{oat}(x_{o}^2, x_{o'}^2) + \sum_{o \in O} x_{o}^2 \right]
\]

s.t. (10) - (15), (17) - (24)
Table 1: Summery of attacks, assets and countermeasures

<table>
<thead>
<tr>
<th>Attacks</th>
<th>Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing</td>
<td>Customers’ personal information</td>
</tr>
<tr>
<td>Keyloggers and spyware</td>
<td>Mobile assets</td>
</tr>
<tr>
<td>Backdoor or command control</td>
<td>Human resources</td>
</tr>
<tr>
<td>Unauthorized access</td>
<td>Anti-virus software</td>
</tr>
<tr>
<td>Packet sniffer</td>
<td>Firewall</td>
</tr>
<tr>
<td>Pretexting</td>
<td>Vulnerability management</td>
</tr>
<tr>
<td>Authentication bypass</td>
<td>Log management software</td>
</tr>
<tr>
<td>Brute-force attack</td>
<td>Forensic tools</td>
</tr>
<tr>
<td>SQL injection</td>
<td>Specialized wireless security</td>
</tr>
<tr>
<td></td>
<td>Public key infrastructure (PKI)</td>
</tr>
<tr>
<td></td>
<td>Encryption</td>
</tr>
<tr>
<td></td>
<td>Intrusion prevention system</td>
</tr>
<tr>
<td></td>
<td>Vulnerability/patch management</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Assets</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Database server</td>
<td></td>
</tr>
<tr>
<td>POS server</td>
<td></td>
</tr>
<tr>
<td>Network devices</td>
<td></td>
</tr>
<tr>
<td>Payment card information</td>
<td></td>
</tr>
</tbody>
</table>

Figure 2: Illustration of the changes in expected total loss as a function of total budget.

4. Policy Analysis based on Practical Data

In this section we implement our cybersecurity investment planning model using data obtained from a representative organization and additional information gathered from the literature. As part of the data gathering process, surveys were performed at the partner organization, where the framework presented was validated from a practical perspective. The surveys also included questions aimed at identifying the distinct categorizations of assets, attacks, and countermeasures as described in Section 2. As noted previously, these high level categorizations were used to allow for identification of general insights applicable to a broad range of situations, as a lower level abstraction of the inputs would imply more of a custom and specific analysis for the organization studied. Based on these data collection efforts, some most common types of assets, attacks, and countermeasures can be listed as shown in Table 1. This information can be considered as being representative of a general cybersecurity implementation, as types of cybersecuriy technologies and other inputs do not show significant differences between industries. Given these categorizations, other input parameters were quantified through the results of the surveys performed, as well as other studies in the literature. We utilize this setup, and obtain several practical insights for firms as described in the following subsections.

4.1 Optimal Total Investment in Cybersecurity

An essential procedure in the decision process of cybersecurity investment is determining budget requirements. As has been emphasized by [5], the total required investment budget needs to be sufficiently discussed and demonstrated before being put into the cybersecurity endeavor. In this section, we conduct a more practice oriented numerical analysis of the optimal budget size based on our data collection. The result is aimed to help the cybersecurity practitioners justify the budget requirement as well as enhance the efficiency of budget utilization.

We first examine the investment for a setup where the affordabilities of different countermeasure types are the same. By gradually relaxing the budget constraint (12) in the model, the objective measured as percentage of the maximum possible total loss takes different values for each budget size. In Figure 2a, we show that there exists a leveling point where increasing the budget will no longer yield further decrease in the objective. In other words, any budget beyond this level is not cost-effective. The budget size at the leveling point is referred to as the optimal budget size.

As the next analysis, we repeat the above process under different setups with the cost of perfect protection varying. The term perfect protection in this context implies that a very high percentage of the maximum possible total loss is avoided. In the experiments, such percentage value is taken to be 99% and is controlled by adjusting the parameter \( \alpha_o \), which is the indicator of the easiness of achieving maximum effectiveness level \( \beta_{o\text{max}} \) for the countermeasure. In
4.2 Impact of Cyber Environment on Budget Allocation

For firms with different business types, the cyber environment they face can be greatly different. A report from Verizon [3] categorize the attack distributions in several businesses, and show that for-profit organizations suffer more advanced attacks then non-profit organizations. The report suggest that firms are better off by focusing more on detections and avoiding overemphasizing preventive measures. This analysis aims to study the trade-offs between investing on detective countermeasures and preventive countermeasure in different cyber environments. By varying the ratio of basic and advanced attack frequencies, we compare the investment level on the two kinds of countermeasures in the outputs.

A visual representation of the experiment result is given in Figure 3a. The vertical axis is the countermeasure investment level in the first stage, and the horizontal axis is the ratio of the frequency of advanced attacks over that of basic attacks. It can be observed that when all other conditions are the same for the two kinds of countermeasures, the trade-off is very obvious: when basic attacks dominate, the firm will invest mostly on detective countermeasures, which is the opposite for the advanced attacks and preventive countermeasure. Another observation is, independent of the investment level of countermeasures going up or down, the trend always follows a concave curve. As a result, the peak of first stage investment occurs when the ratio of advanced/basic attack frequency is between 0.8-1.7. The important insights inherent to the firms here involve that even if attacks are faced with the same frequency, the effort needed to hedge against these attacks can be greatly different. Moreover, a heterogenous cyber environment can be much more dangerous to the firm, and thus requires higher annual or seasonal budget.

Such observations are particularly critical to firms with strong industry features, as some industries are labeled with the importance of their confidential assets and others may consider non-confidential assets as being most essential. [2] studies five typical industries with some significant features, which can also be fit into the paradigm in Figure 3a by considering the ratio of attacks from both categories. Using that framework, we conclude that the financial and the healthcare industries, which experience the most heterogenous cyber environment, are facing the biggest threats among the five; while the retail, hospitality and intellectual property industries are better off with somewhat more homogeneous cyber environment. The conclusion also implies that although experience sharing can be very valuable effort for cybersecurity practitioners, the diversity between different industries definably are non-negligible. Each firm hence should always estimate its own cyber environment when budget allocation is performed.
4.3 Value of Cybersecurity Investment Optimization for Firms

In practice, the key determinants for the protection level of a firm are the maximum potential total loss and costs of perfect protection, while holding the cyber environment and market price of countermeasures stable. This analysis studies the best practice of a firm in terms of the value of applying an optimization model to cybersecurity investment decision problem. The value of optimization in the context refers to the difference between the optimal investment level and that required to achieve a perfect protection as defined in Section 4.1.

In Figure [3b] the value of optimization as a function of the cost of perfect protection is plotted with both values measured relative to the maximum potential loss. As shown, the curve consists of a smooth concave shape with marginal increase diminishing as the cost of perfect protection increases. From the left side of the curve it is observed that as long as the cost of perfect protection is not very low, it is always beneficial to apply an optimization model. With the cost of perfect protection going up, the value of optimization keeps increasing, but at diminishing rates.

We note that the cost of perfect protection, measured in units of the maximum potential loss, is negatively correlated to the size of a firm. It is reasonable to assume that the more powerful the firm, the more abundant the available budget will be. Thus, a smaller firm with less revenues would find it more difficult to cover all the potential losses by achieving the perfect protection level. The conclusion of this analysis implies that strategic budget planning for small sized firms is even more crucial than large firms. Small firms should by no means ignore the management of cybersecurity investment planning. For larger sized firms seeking better cybersecurity endeavors, the result also applies: as the potential losses decrease, the significance of optimization in cybersecurity investment planning should be paid more attention to rather than the other way around. In addition, as the firm grows stronger, it is possible that the potential loss increases or the cost of perfect protection decreases. In that case, the significance of optimization in cybersecurity investment planning should be increased, regardless of the abundance of the available funds.

5. Conclusions and Future Work

In this paper we develop a general framework for cybersecurity investment decision process, and use a stochastic optimization model to identify certain insights for improved budget allocation decisions. It is intended that the proposed framework and modeling will serve as an important step towards a complete approach to practical decision making in this inherently complex and dynamic application area.

References