IPRPD
International Journal of Business & Management Studies
ISSN 2694-1430 (Print), 2694-1449 (Online)
Volume 07; Issue no 01: January, 2026
DOI: 10.56734/ijbms.v7n2a5

A NOVEL INTEGRATED FRAMEWORK FOR MULTI-PERIOD CYBER SECURITY RISK MANAGEMENT

Thomas (Yew Sing) Lee[1]

[1]*Department of Information and Decision Sciences, University of Illinois, Chicago, IL, USA.*

Abstract

Several firms face attacks by multiple types of hackers with type dependent losses during a multiple period planning horizon. It is possible for a hacker that failed to breach the system in a period and decided to try breaching the system again in the next period. At the beginning of the planning horizon, each firm decides on the level of investment for cyber security counter measures. An insurer offers multiperiod cyber insurance coverage to firms with risk averse decision makers. The cyber insurance premium offered depends on the cyber security implemented at the firm. We address the software monoculture issue by assuming that the common or popular software used by all firms is a source of correlated risk. Two types of cyber security interdependence breaching process due to the software monoculture risk were analyzed. For each period, we derive the mean and variance for several performance measures of interest, including the number of breaches. It enables us to develop the multiple period cyber insurance pricing model. We show that the mean and variance for the number of breaches and our pricing formula converge to the long run averages geometrically. We demonstrate the usefulness of our model through numerical examples.

Keywords

Multiperiod Cyber Insurance, Hacker, Number of Breaches, Breaching Probability, Cyber Security, Correlated Risks, Software Monoculture Risk, Multiperiod Integrated Risk Management Strategy

1. Introduction

Our life is fully intertwined with the internet of things, a catch-all term for the billions of smart devices connecting our world: speakers, thermostats, wristwatches, and other devices that are connected to the internet. The ever-growing dependence of individuals and businesses on digital technology has made the threat and potential cost of cyber-attacks ubiquitous and persistent. It is not surprising that the need to protect confidential information is a real and growing concern for individuals as well as at the highest levels of government and industry. That's where cybersecurity comes in. However, cybersecurity is more than just about keeping computer systems and electronic data safe. The CrowdStrike disruption stemmed from a defect found in a single content update for Microsoft Windows hosts causing global tech outage in July 2024, shows the effects of a system failure (July 19, 2024, Reuters). Cybersecurity aims to protect devices, networks, software and data from internal or external cyber threats. Getting hacked isn't just a direct threat to the confidential data companies need. It can also ruin their relationships with customers and even being sued for negligence (e.g., Australia regulator sues FIIG Securities for cybersecurity failures, March 13, 2025, Reuters).

It feels like we hear about a new type of cyber fraud targeting individuals or businesses every day. Thieves steal customer social security numbers from corporations' computer systems. Unscrupulous hackers grab passwords and personal information from social media sites or pluck company secrets from the cloud. Furthermore, Artificial intelligence (AI) is making it easier for hackers to send out many

phishing emails. These emails have perfect grammar and are often more convincing than those written by the hackers themselves. The reality is that AI allows attackers to generate thousands of unique and high-quality phishing emails in seconds. These AI generated emails can perfectly mirror someone's writing style, or they can discuss a real project that's being worked on. VIPRE's Email Threat Trends Report 2024 have found that 40% of all phishing emails are now generated by AI and Heiding et al 2024 found that 60% of people who receive an AI generated phishing email fall for it. Furthermore, it has been reported that from November 2021 to October 2022, Microsoft Office applications were the most exploited applications worldwide at 70% (Sobers, 2023; Petrosyan, 2023).

It should be recognized that cyber-attacks are not new as they have been happening for decades. As we have become more dependent on digital technology and infrastructure, created more value in digital assets and more usage of the Internet, then the potential for harm resulting from cyberattack has grown significantly. Furthermore, the cybersecurity business is a loaded game, and it favors the attackers. The cost for hackers to launch attacks is much cheaper than the cost for firms to defend against such attacks. Even the very modest resources of the attackers can create huge threats to firms trying to fend off potential attacks, despite the latter's extensive monetary and technical resources. Therefore, it is not surprising to see that the annual cybersecurity spending continues to grow despite ongoing macroeconomic uncertainty and constrained IT budgets. For example, Gartner reported that the annual cybersecurity spending worldwide is $193 billion in 2024; projected to reach $213 billion in 2025 and estimated to grow to $240 billion in 2026.

We also must recognize that we don't live in a perfect world and perfect defense against cyber-attacks doesn't exist. Therefore, we must accept a level of risk, a residual risk that exists even after we have deployed our best defenses. Being cyber-secure means accepting a level of insecurity but attempting to manage it so we can survive should the worst happen. Therefore, cyber-risk is a risk that must be managed, and to do that we must understand the nature of the cyber risks that we face. Therefore, if a hacker gets into the system, the company needs a tested incident response plan to help regain control of their networks and minimize the damage.

Insurers play a critical role in ensuring businesses are prepared to respond to cyber-attacks. Not only do they provide financial support, but they also have partnerships with security vendors and experts who can help businesses quickly recover. These tools are especially useful for smaller businesses. Small and medium-sized companies might not have their own IT security department, they might not have their own troubleshooter, so they tend to rely more on services that are offered by cyber insurance. A well-designed cyber insurance policy could reduce the number of cyber-breaches by incentivizing the adoption of preventative/counter measures in return for more coverage and the implementation of best practices by basing premiums on an insured implemented level of cyber security self-protection. On the other hand, a poorly designed cyber insurance program could shift too much risk to the insurer and reduce firms' incentives to shore up cybersecurity. In practice, more organizations are buying cyber insurance for the first time or are expanding it as cyber insurance has been gaining increasing acceptance among firms. This market is growing as more insurers are adding cyber insurance policies with higher limits to their offerings. The customers also want cyber insurance to provide broader coverage. For example, the growing need to cover business interruption and contingent business interruption risks is due to expanding dependence on technology. This is a significant market driver for cyber insurance as traditional business interruption coverage generally does not cover losses when cyber incidents are the cause. However, estimating the premium continues to be a significant challenge in cybersecurity insurance. This requires that insurers understand the probability of a breach or the number of breaches occurring. Estimating the probability of a breach or the number of breaches occurring is complex and is based on a few factors. Cybersecurity breaches tend to be correlated across firms in the same industry. The probability of a breach or the number of breaches occurring also depends upon the amount of resources the firm deploys in its IT security budget. Other factors include whether the firm is diversified in its use of software.

Section 1.1: Related Work

In this subsection, we present an overview/grouping of existing research papers that are related to our research topic. There is a line of research in the economics of information security that is of interest to us. The most established model to relate optimal security investments and vulnerability reduction is due to Gordon and Loeb (Gordon and Loeb 2002). Specifically, a firm needs to determine the most effective level of information security investment, based on the nature of the information sets it intends to protect, the vulnerability of its information systems, the potential loss associated with a security breach if it does occur,

and the security environment that it faces. This is a single firm, single event, single-period model. The authors show that there exists an optimal level of security investment for a given security vulnerability and threat environment of each organization. Investing less than that optimal level will result in unacceptable security risks; on the other hand, investments exceeding the optimal level do not bring justifiable returns for the investment. Mazzoccoli and Naldi 2022 also provide an extensive literature review for the topic of interest. For additional references, see Huang et al 2008; Gordon et al 2012; Chong et al. 2022.

Another line of research of interest deals with cybersecurity investment strategies for firms facing attacks (see Wu et al 2015; Zhuo and Solak 2014; Mayadunne and Park 2016, Naldi et al 2018; Mazzoccoli and Naldi 2021). The methodology used to analyze the issue including game theory, decision analysis, and stochastic programming.

A third line of research of interest is about analyzing cyber insurance. Marotta et al. 2017 conducted an excellent survey of cyber insurance models. Furthermore, various approaches have been developed for computing insurance premiums (see Franke 2017 and Strupczewski 2018, Mukhopadhyay et al. 2019; Naldi and Mazzoccoli 2018 and Mazzoccoli and Naldi 2020b; Rosson et al. 2019; Khalili et al. 2018; Mastroeni et al. 2019).

The fourth line of research combines vulnerability reduction investments with insurance coverage for residual risk. A number of papers have extended the Gordon and Loeb model to incorporate insurance in critical infrastructure cyber risk strategies (see Young et al 2016; Xu et al. 2019; Mazzoccoli and Naldi 2020; Mazzoccoli and Naldi 2021). Mazzoccoli and Naldi 2022 deal with the problem of computing the optimal balance between investment and insurance payments to achieve the minimum overall security expense when the vulnerability grows over time according to a logistic function. Mazzoccoli 2023 reveals that the insurance premium tends to be the dominant component in the overall security expense in most cases which implies that the cost of insurance outweighs the cost of security investments. It is important to highlight that the security breach function plays a critical role in this line of research. This function describes the impact of investments on the probability of a successful attack. Modeling vulnerability through the security breach probability function satisfies the risk description step as it provides a probability value (Aven 2011, Aven and Flage 2020 and Hausken 2006). It also enables risk evaluation by computing the expected value of losses associated with breach events. Therefore, choosing an appropriate model for the security breach probability function is a fundamental step in probabilistic risk assessment for this line of research. Lee 2025 introduces a stochastic single period model to analyze the effects of using insurance to incentives firms facing correlated risks to invest in cybersecurity. Using a new modeling framework, Lee derives the breaching probability distribution without having to assume a particular functional form for the security breach function. The optimal cyber insurance for each firm is formulated as a nonlinear integer programming optimization problem. However, Lee's static model does not allow the possibility that the hacker failed to breach the system and decided to try again in the next period.

All the aforementioned research deals with single period models. A fifth line of research recognized the shortcoming of the single period model and dealt with multiple period models. David et al 2018 argued that a single-period model is not adapted to capture dynamic aspects of information security investment such as the advent of disruptive technology. The extension to a multi-periods model is indeed necessary. Furthermore, the security breach probability function of the original Gordon and Loeb model could not be considered as continuously differentiable in the context of the introduction of a discrete radically innovative information security technology. David et al 2018 propose an extension of the Gordon-Loeb model by considering multi-periods and relaxing the assumption of a continuous security breach probability function. Like Gordon and Loeb model, their method requires an explicit assumption of the functional form of the security probability breach function. Another dynamic extension of Gordon and Loeb model has been proposed by Krutilla et al 2021. This is a deterministic model and like Gordon and Loeb model they assume a specific functional form for cybersecurity breach function. Mazzoccoli and Naldi 2022 deal with the problem of computing the optimal balance between investment and insurance payments to achieve the minimum overall security expense when the vulnerability grows over time according to a logistic function. Callegaro et al 2025 proposed a continuous-time stochastic Gordon-Loeb model for optimal cybersecurity investment under clustered attacks.

1.2. Motivation and Our Contribution

Our research question is three-fold. First, how should insurance companies' price multiperiod cybersecurity insurance premiums to manage their exposure in this market (i.e., in a dynamic environment where multiple types of breaches among firms are often correlated)? Second, how can insurance

companies offer multiperiod cyber insurance contracts that incentivize the firm to implement the best practices or invest appropriately in cyber security? Third, how can we model the loss cost of the firm over multiple periods, which includes not only the direct costs of a breach, but the harder-to-estimate indirect costs that harm the value of the firm, such as loss of reputation, disruption of operations, etc.

This paper aims to extend current research in dynamic integrated risk management strategy, combining insurance and cyber security investments, where the latter contributes to reducing the insurance premium over a multiple period planning horizon. It is understood that the term period meant a time duration of interest (e.g., day, week, month or year). Our model assumes a multiperiod planning horizon where the firm's decision maker is risk averse and intends to use cyber insurance to deal with cyber risks. We show that the cyber insurer's risk pooling process does reduce risk for individual firms even with correlated risk across firms. We also provide theoretical justification for our cyber insurance pricing formula. Comparative statics analysis shows that the proposed pricing formula confirms our intuition that cyber insurance prices would increase if the variability of loss, number of hackers/attacks or breaching probabilities increases. Utilizing our pricing model, we determine the firm's optimal level of investment for cyber security. The main difference between our approach and existing research are as follows. First, the optimal information security problem is based on a static or one period model. We introduce a new multiperiod discrete-time stochastic model to study a dynamic integrated risk management strategy, combining insurance and cyber security investments, where the latter contributes to reducing the insurance premium over the multiperiod planning horizon. Our multiple period/discrete-time stochastic model allows us to analyze the effects of a hacker who failed to breach the system in a period but decided to try to breach the system again next period while it is not possible to model the retrial hacker in a static or one period model. We define the cyber security investment cost function as a discrete cost function of implemented cyber security level which is a more accurate representation of the observed discrete cyber-investment cost curve in practice. For each period, we derive the mean and variance of the total cost function. Our method allows us to show that the per period performance measures converge to the long run averages geometrically. Secondly, a firm's loss cost may not be deterministic because different types of cyber-attacks or breaches (e.g., malware, Code Injection Attacks, Denial-of-Service Attack, SQL Injection Attack, etc.) may lead to different recovery times and hence costs. By allowing for the possibility of random hacker dependent loss cost, we capture the dependence of loss costs on the type of cyber-attacks and recovery time. Our method requires us to know the first two moments of the firm's loss cost. In practice, this flexibility allows us to utilize any available statistical methodologies that only uses the first two moments to estimate losses. Thirdly, each firm faces attacks by multiple types of hackers or threats. Our analysis allows the number of hackers or threats to be correlated. It enables us to model the software monoculture risk (Sobers, 2023; Petrosyan, 2023). We explicitly model the security system of the firm as a finite discrete multi-level system. Furthermore, the breaching probability for each firm is not necessarily the same and it also depends on the type of hacker initiating the cyber-attack. Our model includes the plausibility of security interdependence. We analyze two cases of security interdependence; where a hacker breaches a firm then it breaches all firms and the case where a hacker breaches a firm then it does not necessarily breach all firms. For each period, we were able to derive the mean and variance of the number of hackers breaching the system as a function of the type of hacker and the security level deployed by the firm. We capture a more realistic decision-making process by taking into consideration the multiple types of correlated hackers, and security level deployed by individual firms. Finally, we noticed that cyber-attacks may not be rare events but in comparison, cyber breaches are not as common. Therefore, we believe that expected cost is not an appropriate measure for evaluating different strategies for managing cyber risks. Our approach allows us to capture the trade-off between mean and variability. This is the trade-off that our model can capture whereas models that are based on mean cost would not be able to. Consequently, our model would offer valuable managerial insight into how firms with risk-averse decision makers should make decisions regarding using cyber insurance as part of their program in dealing with cyber security risks as well as its own investment in information and system security. Thus, instead of directly comparing the expected cost and expected benefits of cyber security investment, we analyze the optimal cyber security investment level using a different approach (e.g., mean-standard deviation analysis). Lastly, our approach differs significantly from the existing literature in that we do not assume a particular functional form for the security breach function. Rather, our approach derives performance measures of interest as a byproduct of our modeling framework without assuming a specific functional form for security breach function.

The remainder of this paper is organized as follows. We introduce a multi-firm, multiple-event, multiple-period cyber security breach model in section 2. Our model allows the possibility of correlated cyber breaches across firms and the possibility for hackers who failed to breach the system in a period to retrial again next period. Section 3 analyzes the model introduced in section 2. We analyzed two types of security interdependence breaching process. The first type of security breaching process indicates that if a hacker breaches a firm, then it breaches all firms. The second type of security breaching process indicates that if a hacker breaches a firm, it is not necessary that it breaches all firms. We derive the mean and variance for several performance measures of interest including the number of breaches for a given period and the number of hackers failed to breach the system but decided to try again next period. We also show that the mean and variances of several performance measures approach the long run average with geometric convergence rate. Section 4 describes our cyber security investment cost model and the losses resulted from cyber-attacks. We show that by pooling the risk faced by the individual firm the insurer can reduce the individual firm's risk even with the presence of correlated risks. We also show that correlated hackers arrival process increases the variance of the cost function. Section 5 introduces our cybersecurity insurance pricing model. Using our cybersecurity pricing formula, the optimal cyber security investment problem is formulated as a non-linear integer programming optimization problem. We also provide some theoretical and numerical results. The last section concludes and provides future directions for research. Appendix collects the proof of our results.

2. The Hacker's Model

We aim to develop a multi-firm, multiple-event, multiple-period stochastic cyber security breach model. It is understood that the term period meant a time duration of interest (e.g., day, week, month or year). In this paper, we consider an insurer's portfolio of w firms (policyholders) exposed to the considered type of cyber risk incidents. We define cyber-attack as when there is an unauthorized system/network access by a third party. The person who carries out a cyberattack is termed as a hacker or threat. Throughout this paper, we will use the term hacker and threat interchangeably. Let $T=\{s,1,2,\ldots,h\}$ be the set of all possible threats and let $T_k \in T$ be the set of threats or hackers face by firm k for $k = 1,\ldots,w$. Effectively, we assume that each firm k must deal with $|T_k|$ types of hackers. For each $i \in T_k$, let $A_{ki}(t)$ denote number of type i hackers attack firm k during period t; $t \geq 1$. We assume that $A_{ki}(t)$ is a Poisson random variable with parameter λ_{ki} and $\{A_{ki}(t);$ all t, k and $i\}$ are independent random variables. Then, the total number of hackers attack firm k during period t is given by

$$A_k(t) = A_{ks}(t) + \sum_{i \in T_k \setminus \{s\}} A_{ki}(t). \quad (1)$$

To model the software monoculture risk (Sobers, 2023; Petrosyan, 2023), we assume that there is a *special* type of software that is used by all firms. Therefore, we assume that $s \in T_k$ for all $k = 1,\ldots,w$. In particular, we differentiate type s hacker from other types of hackers to model the software monoculture risk. Specifically, type s hacker attacks all w firms simultaneously upon arrival. While other (i.e., non-special) types of hackers/threats attack only one firm upon arrival. By definition $A_{ks}(t) = A_{js}(t)$ for all $k,j=1,2,\ldots,w$; $t \geq 1$ and $A_{ks}(t)$ is a Poisson random variable with parameter $\lambda_{ks} \equiv \lambda_s$. From equation (1), we get

$$A_k(t) = A_{1s}(t) + \sum_{i \in T_k \setminus \{s\}} A_{ki}(t) \text{ for all } k = 1,\ldots,w. \quad (2)$$

Remark 1: In this paper**,** we will use equation (1) with the assumption that $\{A_{ks}(t); 1 \leq k \leq w\}$ are independent and identically distributed Poisson random variables with parameter $\lambda_{ks} = \lambda_{1s} = \lambda_s$ to represent the case of independent (i.e., without software monoculture) risks.

Remark 2: For ease of exposition, we choose type s as the only type of hackers that attack all firms upon arrival. Our model allows one to deal with multiple types of hackers that attack a subset of firms upon arrival.

The cyber-security counter measures implemented by a firm are usually a function of the budget allocated or investment in cybersecurity. Examples of cyber-security counter measures include identity management and access control, installing anti-malware and anti-phishing software, managing the

inventory of authorized and unauthorized devices and software, patch management, setting up a network and/or application firewalls, training of staff against social engineering attacks, data back-up and resource redundancies, physical security, etc.

Let us denote the set of all available counter measures is $U = \{0,1,2,\dots,u\}$ and let $U_k \subseteq R$ be the set of counter measures considered for implementation by firm k for $k = 1,\dots,w$. We order the counter measures so that level 0 is the simplest (or least costly) and level $|U_k|$ is the most complex (or most expensive). One can interpret level 0 as no or minimum level counter measure implemented by firm *k* and level *u* as the firm implemented *all* available counter measures. We have three practical reasons for imposing the upper bound *u* on the maximum level of cyber security implemented. The first practical reason is due to the limited or available budget for cyber security investment. The second practical reason for imposing this upper bound is the negative side effects on the normal operation of an organization. Some examples of the negative side-effect include the downtime of a database server for applying a patch, every time an employee who gets a new digital device would need to spend time and go through the appropriate channel to gain access to the system, or the slowdown of network caused by an application proxy. The third practical reason for imposing this upper bound is that there is no perfect defense against cyber-attacks because new type of cyber-attacks (e.g., virus, malware, Code Injection Attacks, Denial-of-Service Attack, phishing, SQL Injection Attack, etc.) continue to pop up as time progresses. Therefore, we will always need to live with a certain amount of residual risk even after we have deployed *all* available counter measures.

To model the impact of hackers, we assume that at the end of every period, there are three possible mutually exclusive outcomes for each hacker: (i) the hacker successfully breached the firm's security system; (ii) the hacker failed to breach the firm's security system and decided to leave; and (iii) the hacker failed to breach the firm's security system but decided to try again next period.

Let us define m_k as the level of counter measures implemented by firm *k*; let $\beta_i(m_k)$ the probability that a type *i* hacker successfully breach firm *k* during period *t;* let d_{ki} the probability that a type *i* hacker fail to breach firm *k* and depart or leave the system during period *t;* and let r_{ki} the probability that a type *i* hacker fail to breach firm *k* the system during period *t* and decide to try again next period. We have by definition for all *k* and *i*;

$$\beta_i(m_k) + d_{ki} + r_{ki} = 1; \quad 0 \le \beta_i(m_k) \le 1, \quad 0 \le r_{ki} \le 1; \quad 0 \le d_{ki} \le 1.$$

For each period *t*, $t \ge 1$; let us define $Q_{ki}(t)$ as the number of type *i* hackers attack firm *k at the beginning of* period *t;* let $D_{ki}(t)$ denote the number of type *i* hackers attack firm *k* during period *t* decided to leave the system without breaching the system; let us define $B_{ki}(t)$ is the number of type *i* hackers successfully breached the firm *k*'s security system during period *t* and let $R_{ki}(t)$ be the number of type *i* hackers failed to breach the firm *k*'s security system during period *t* but decided to try again next period.
With these notations, for each *k*, *i* and *t;* we have the following flow balance equation,

$$Q_{ki}(t+1) = Q_{ki}(t) + A_{ki}(t) - D_{ki}(t) - B_{ki}(t) = R_{ki}(t). \qquad (3)$$

The first equality follows easily from the conservation of mass principal. The second equality follows from noticing that the only way that a hacker is in the system during period *t* would still remain in the system during the next period if and only if the hacker failed to breach the firm *k*'s security system during period *t* and decided to try again next period (i.e., $R_{ki}(t)$ is the part of $Q_{ki}(t) + A_{ki}(t)$ that remains in the system at the end of the period).

Remark 3: Suppose that for each *k*, *i* and *t;* $R_{ki}(t) \equiv 0$. Thus, every hacker failed to breach the security system would leave the system at the end of the period. In this case*;* our multiple periods problem becomes multiple (identical) copy of the 1 period problem analyzed in (Lee 2025).

Noticed that for each *k*, *i* and *t;* given $Q_{ki}(t) + A_{ki}(t)$ we have $(B_{ki}(t), D_{ki}(t), R_{ki}(t))$ is a multinomial random variable with parameters $Q_{ki}(t) + A_{ki}(t)$ and $(\beta_i(m_k), d_{ki}, r_{ki})$. Therefore, we have

$$E\{B_{ki}(t)|Q_{ki}(t) + A_{ki}(t)\} = \beta_i(m_k)(Q_{ki}(t) + A_{ki}(t)); \qquad (4.1)$$
$$Var\{B_{ki}(t)|Q_{ki}(t) + A_{ki}(t)\} = \beta_i(m_k)(1 - \beta_i(m_k))(Q_{ki}(t) + A_{ki}(t)); \qquad (4.2)$$
$$E\{D_{ki}(t)|Q_{ki}(t) + A_{ki}(t)\} = d_{ki}(Q_{ki}(t) + A_{ki}(t)); \qquad (4.3)$$

$$Var\{D_{ki}(t)|Q_{ki}(t)+A_{ki}(t)\} = d_{ki}(1-d_{ki})(Q_{ki}(t)+A_{ki}(t)); \quad (4.4)$$

$$E\{R_{ki}(t)|Q_{ki}(t)+A_{ki}(t)\} = r_{ki}(Q_{ki}(t)+A_{ki}(t)); \quad (4.5)$$

$$Var\{R_{ki}(t)|Q_{ki}(t)+A_{ki}(t)\} = r_{ki}(1-r_{ki})(Q_{ki}(t)+A_{ki}(t)); \quad (4.6)$$

$$Cov\{R_{ki}(t), D_{ki}(t)|Q_{ki}(t)+A_{ki}(t)\} = -r_{ki}d_{ki}(Q_{ki}(t)+A_{ki}(t)); \quad (4.7)$$

$$Cov\{B_{ki}(t), D_{ki}(t)|Q_{ki}(t)+A_{ki}(t)\} = -d_{ki}\beta_i(m_k)(Q_{ki}(t)+A_{ki}(t)); \quad (4.8)$$

$$Cov\{R_{ki}(t), B_{ki}(t)|Q_{ki}(t)+A_{ki}(t)\} = -r_{ki}\beta_i(m_k)(Q_{ki}(t)+A_{ki}(t)). \quad (4.9)$$

To develop a model to analyze $B_{ki}(t)$; the number of type *i* hackers successfully breached the firm *k*'s security system during period *t*, let $Б_{kvij}(t)$ denote the indicator random variable associated with the event of v^{th}type *i* hacker successfully breach counter measures level *j* of firm *k* during period *t;*

$$Б_{kvij}(t) = \begin{cases} 1 & \text{if the } v^{th}\text{type } i \text{ hacker breach counter measures level } j \text{ of firm } k \text{ during period } t, \\ 0 & otherwise \end{cases}$$

and let us define

$$P\big(Б_{kvij}(t)=1\big) = \beta_{ij};\ 0 \le \beta_{ij} \le 1 \text{ for all } t, k, i, j \text{ and } v.$$

Noticed that $\beta_{ij} = 0$ represents the case of perfect counter measures. In practice, we know that perfect counter measures don't exists and hence we have $0 < \beta_{ij}$.

We assume that $\{Б_{kvij}(t);$ all t, k, v, i and $j\}$ are independent random variables. Next, we can define the indicator random variable to represent the event where the v^{th} type *i* hacker breach all counter measures implemented by firm *k* during period *t* as $\prod_{j=0}^{m_k} Б_{kvij}(t)$ where we recall m_k is the level of counter measures implemented by firm *k*. By definition, we have the probability that a type *i* hacker successfully breach firm *k* during period *t* as

$$\beta_i(m_k) \equiv P\Big(\prod_{j=0}^{m_k} Б_{kvij}(t)=1\Big) = \prod_{j=0}^{m_k} P(Б_{kvij}(t)=1) = \prod_{j=0}^{m_k}\beta_{ij}. \quad (5)$$

Remark 4 (Property of the probability $\beta_i(m_k)$)

(a): If $\beta_{ij} = 0$ for some *j* then $\beta_i(m) = 0$ for all $m \ge j$. Thus, we see that if a system is not vulnerable (i.e., has a perfect counter measures) to type *i* hacker attacks, then it will remain not vulnerable regardless of the additional level of security implemented/investment beyond the perfect counter measure implemented (i.e., the ideal case).

(b) $\beta_i(0) = \beta_{i0}$. Thus, we see that if there is no investment in additional security controls, then there is no change in the likelihood of a successful breach.

(c) The breach probability $\beta_i(m)$ is a decreasing function of the firm's security investment. That is $\Delta\beta_i(m) = \beta_i(m+1) - \beta_i(m) = (\beta_{i,m+1} - 1)\beta_i(m) \le 0$ for all $m \ge 0$. Therefore, the system is made more secure as the level of cyber security implemented/invested; m_k increases. We also have $\Delta^2\beta_i(m) = \beta_i(m+2) - 2\beta_i(m+1) + \beta_i(m) = \beta_i(m)\{1 - 2\beta_{i,m+1} + \beta_{i,m+2}\}$. So we see that $\beta_{i,j+1} \ge 2\beta_{ij} - 1$ for all i, j implies that $\Delta^2\beta_i(m) \ge 0$. Noticed that if there is no limit of the level of counter measures the firm can employed then one have $\lim_{m_k\to\infty} \beta_i(m_k) = 0$.

It implies that we can implement or invest in an adequate level of cyber security and the probability of a successful breach can be made arbitrarily close to zero. By definition *u* is the maximum level of countermeasure available for implementation and $\beta_i(u) = \prod_{j=0}^{u}\beta_{ij}$ represent the *residual risk* due to type *i* hacker that the firm must accept even after *all* available counter measures have been deployed.
With the above notations, we can write $B_{ki}(t)$ is the number of type *i* hackers successfully breached the firm *k*'s security system during period *t* as

$$B_{ki}(t) = \sum_{v=1}^{Q_{ki}(t)+A_{ki}(t)} \prod_{j=0}^{m_k} Б_{kvij}(t) \quad (6)$$

and we have $B_k(t)$ is the number of hackers successfully breaching the firm k's security system during period t (i.e., the total number of security breaches) as

$$B_k(t) = \sum_{i \in T_k} B_{ki}(m_k, t). \quad (7)$$

3. Mean-Variance Analysis

In this section, we consider the issue of multi period cyber security interdependence. For any time period t, we will derive the mean and variance for the performance measures of interest such as the number of hackers successfully breaching the firm in each period and the number of hackers failing to breach the security system during a period but decided to try again during the next period. We start with the following result on the number of hackers in the system at the beginning of each period t; $Q_{kj}(t)$.

Theorem 1: For any k, j and initial value of $Q_{kj}(1)$; we have for $t \geq 1$

$$E\left(Q_{kj}(t+1)\right) = E\left(Q_{kj}(1)\right)(r_{kj})^t + r_{kj}\lambda_{kj}\frac{1-(r_{kj})^t}{1-r_{kj}}; \quad (8)$$

$$Var\left(Q_{kj}(t+1)\right) = (r_{kj}^2)^t Var\left(Q_{kj}(1)\right) + E\left(Q_{kj}(1)\right) r_{kj}^t\left(1-r_{kj}^t\right) + r_{kj}\lambda_{kj}\left(\frac{1-(r_{kj})^t}{1-r_{kj}}\right); \quad (9)$$

$$Cov\left(Q_{ks}(t+1), Q_{js}(t+1)\right) = (r_{ks}r_{js})^t Cov\left(Q_{ks}(1), Q_{js}(1)\right) + r_{ks}r_{js}\lambda_s\left(\frac{1-(r_{ks}r_{js})^t}{1-r_{ks}r_{js}}\right);\ k \neq j \quad (10)$$

For ease of exposition the proof of our results is placed in the appendix. Given the initial value of the number of type i hackers attack firm k *at the beginning of* period *1*, Theorem 1 provides us with the mean, variance and covariance of the number of hackers in the system at the beginning of each period during our multiple periods planning horizon. Utilizing this result, we get

Theorem 2: For any k, j and initial value of $Q_{kj}(1)$; for $t \geq 1$ we have

$$E\left(R_{kj}(t)\right) = E\left(Q_{kj}(1)\right)(r_{kj})^t + r_{kj}\lambda_{kj}\frac{1-(r_{kj})^t}{1-r_{kj}}; \quad (11)$$

$$Var\left(R_{kj}(t)\right) = r_{kj}^{2(t)} Var\left(Q_{kj}(1)\right) + r_{kj}^t\left(1-r_{kj}^t\right)E\left(Q_{kj}(1)\right) + r_{kj}\lambda_{kj}\left(\frac{1-(r_{kj})^t}{1-r_{kj}}\right); \quad (12)$$

$$E\left(B_{kj}(t)\right) = \beta_j(m_k)(r_{kj})^{t-1}E\left(Q_{kj}(1)\right) + \beta_j(m_k)\lambda_{kj}\frac{1-(r_{kj})^t}{1-r_{kj}}; \quad (13)$$

$$Var\left(B_{kj}(t)\right) = \beta_j(m_k)^2({r_{kj}}^2)^{t-1}Var\left(Q_{kj}(1)\right) + r_{kj}^{t-1}\beta_j(m_k)\left(1-r_{kj}^{t-1}\beta_j(m_k)\right)E\left(Q_{kj}(1)\right) + \beta_j(m_k)\lambda_{kj}\left(\frac{1-(r_{kj})^t}{1-r_{kj}}\right) \quad (14)$$

$$E\left(D_{kj}(t)\right) = d_{kj}(r_{kj})^{t-1}E\left(Q_{kj}(1)\right) + d_{kj}\lambda_{kj}\frac{1-(r_{kj})^t}{1-r_{kj}}; \quad (15)$$

$$Var\left(D_{kj}(t)\right) = {d_{kj}}^2({r_{kj}}^2)^{t-1}Var\left(Q_{kj}(1)\right) + r_{kj}^{t-1}d_{kj}\left(1-r_{kj}^{t-1}d_{kj}\right)E\left(Q_{kj}(1)\right) + d_{kj}\lambda_{kj}\left(\frac{1-(r_{kj})^t}{1-r_{kj}}\right); \quad (16)$$

$$Cov(B_{ks}(t), B_{is}(t)) = \beta_s(m_k)\beta_s(m_i)(r_{ks}r_{is})^{t-1}Cov\left(Q_{ks}(1), Q_{is}(1)\right) + \lambda_s\beta_s(m_k)\beta_s(m_i)\frac{1-(r_{ks}r_{js})^t}{1-r_{ks}r_{is}};\quad k \neq i. \quad (17)$$

Theorems 1 & 2 describe the dynamics of the system from period to period. It provides us with a way to compute for each period, the mean, variance and covariance to calculate several performance measures of

interest to us. With theorem 2, we can compute the mean and variance of the number of hackers successfully breaching the firm *k*'s security system during period *t* (i.e., the total number of security breaches). The following corollary follows immediately from theorem 2.

Corollary 1: For any *k*, *j* and initial value of $Q_{kj}(1)$; for $t \geq 1$ we have

$$E(B_k(t)) = \sum_{i \in T_k} \beta_j(m_k)(r_{kj})^{t-1} E\left(Q_{kj}(1)\right) + \beta_j(m_k)\lambda_{kj}\frac{1-(r_{kj})^t}{1-r_{kj}}$$

$$Var(B_k(t)) = \sum_{i \in T_k} \{\beta_j(m_k)^2 (r_{kj}{}^2)^{t-1} Var\left(Q_{kj}(1)\right) + \sum_{i \in T_k} r_{kj}^{t-1}\beta_j(m_k)\left(1 - r_{kj}^{t-1}\beta_j(m_k)\right) E\left(Q_{kj}(1)\right) + \beta_j(m_k)\lambda_{kj}\left(\frac{1-(r_{kj})^t}{1-r_{kj}}\right)\}.$$

Utilizing theorem 1&2, the following result shows the geometric convergence of the mean and variance of the performance measures of interest to the long run or steady state value.

Theorem 3: For any *k*, *j* and initial value of $Q_{kj}(1)$; as $t \to \infty$ we have

$$E(Q_{kj}) = Var(Q_{kj}) = E(R_{kj}) = Var(R_{kj}) = \frac{r_{kj}\lambda_{kj}}{1-r_{kj}}; \quad (18)$$

$$E(B_{kj}) = Var(B_{kj}) = \frac{\beta_j(m_k)\lambda_{kj}}{1-r_{kj}}; \quad (19)$$

$$E(D_{kj}) = Var(D_{kj}) = \frac{d_{kj}\lambda_{kj}}{1-r_{kj}}; \quad (20)$$

$$Cov(Q_{ks}, Q_{js}) = \frac{r_{ks}r_{js}\lambda_{1s}}{1-r_{ks}r_{js}}; \quad k \neq j; \quad (21)$$

$$Cov(B_{ks}, B_{js}) = \frac{\lambda_{1s}\beta_s(m_k)\beta_s(m_j)}{1-r_{ks}r_{js}}; \quad k \neq j. \quad (22)$$

Theorem 3 specifies the *steady state* mean and variance of the performance measures of interest. Moreover, the rate of convergence is geometric and depends on the retrial rate r_{kj}.

Example 1: Suppose, $r_{kj} = r_{ks} = r_{js} = 0.5$ *and* $t = 12$ then we have $r_{kj}{}^{12} = (0.5)^{12} = 0.000244$ and $(r_{ks}r_{js})^{12} \approx 0$. Thus, we see that for a *12* period planning horizon, $E(X_{kj}) - E\left(X_{kj}(t)\right) \approx 0$; $Var(X_{kj}) - Var(X_{kj}(t)) \approx 0$; and $Cov(X_{ks}, X_{js}) - Cov(X_{ks}(t), X_{js}(t)) \approx 0$ where $X_{kj} \in \{Q_{kj}, B_{kj}, R_{kj}, D_{kj}\}$.

It is important to realize that Theorem 3 does not say that $(Q_{kj}(t), B_{kj}(t), R_{kj}(t), D_{kj}(t))$ reach steady state distributions. They might. Our interest focuses on their mean, variance and covariance.
The following corollary follows immediately from theorem 3 and corollary 1. It shows the geometric convergence of the mean and variance of the total number of security breaches to the long run or steady state value.

Corollary 2: For any *k*, *j* and initial value of $Q_{kj}(1)$; as $t \to \infty$ we have

$$E(B_k) \equiv \lim_{t\to\infty} E(B_k(t)) = \sum_{j \in T_k} \frac{\beta_j(m_k)\lambda_{kj}}{1-r_{kj}} \;\&\; Var(B_k) \equiv \lim_{t\to\infty} Var(B_k(t)) = \sum_{j \in T_k} \frac{\beta_j(m_k)\lambda_{kj}}{1-r_{kj}}.$$

The above corollary justifies our intuition that the total number of security breaches is an increasing function of the hacker's arrival rate, hacker's retrial rate and the breaching probability.

4. Cost Model

Each firm admits an individual risk profile characterized by several factors, e.g., potential loss, *IT security level implemented*, etc. Depending on the available budget, each firm has incentive to invest in cyber security or implement certain levels of counter measures to avoid cyber security breaches as loss due to cyber security breaches is costly. Let us define cyber security investment cost as the amount of money spent to enhance cybersecurity within a given period with the expectation of reducing financial loss due to cyber security breaches. In practice the cyber-investment cost curve is a discrete cost curve with a specified defense probability range (i.e., not the entire range between 0 and 1 as there is no perfect defense). This observation motivates us to define the cyber security investment cost function as a discrete cost function of implemented cyber security level. Let us denote firm *k*'s cost of security investment for maintaining countermeasure level *m* during period *t* as $g_k(m,t)$. We assume that $g_k(m,1)$ is a strictly increasing function of *m*; $g_k(m,t)$ is an increasing function of *m* and independent of *t*. That is $g_k(m,t)$ satisfies

$$\Delta g_k(m,1) \equiv g_k(m+1,1) - g_k(m,1) > 0 \text{ and } \Delta g_k(m,t) \equiv g_k(m+1,t) - g_k(m,t) \geq 0; \;\; t \geq 2.$$

One can also think of $g_k(m,t)$ as the subscription cost for the cybersecurity software that the firm implemented or more generally the IT security investment during period *t*.

Remark 5(a): (Discrete cyber security investment cost curve) Let $g_k(m,t) = a_{km}$ denote the firm *k*'s cost of implementing level *m* cybersecurity during period *t*. We assume that $\{a_{kj} | 0 \leq a_{kj} < a_{k,j+1} \; for \; all \; 1 \leq k \leq w; 0 \leq j \leq u\}$. That is, higher level of cybersecurity invested/implemented is more costly than lower level of cybersecurity invested/implemented. Two special cases of discrete cost function are the step function and the polynomial cost function.

Remark 5**(b):** (S-curve) An investment cost curve widely used for cost estimation of technology projects is the S-curve or s-shaped curve. Our model allows us to model security investment cost as an S-curve. For a specific example, we can define $g_k(m,t)$ as a logistic function $g_k(m,t) = \frac{z_1}{(1+e^{-z_2(m-z_3)})}$ where $z_1, z_2 \; and \; z_3$ are constants. In practice, we obtain these 3 constants by fitting the cost function into historical data using the multiple linear regression technique.

We let the random variable L_{kvi} denote the loss due to the v^{th}type *i* hacker breach all counter measures of firm *k*. We assume that the period *t* cost function for firm *k;* $C_k(m_k,t)$ can be written as a sum of security investment cost $g_k(m)$ and the period *t* loss cost

$$C_k(m_k,t) = g_k(m,t) + \sum_{v=1}^{B_{ks}(t)} L_{kvs}(t) + \sum_{i \in T_k \setminus \{s\}} \sum_{v=1}^{B_{ki}(t)} L_{kvi}(t) \qquad \text{for all } k \text{ and } t. \tag{23}$$

By hypothesis, we assume that there is at least one type of software that is used by all firms. We differentiate type *s* hacker from other types of hackers to model the software monoculture risk. Specifically, type *s* hacker attacks all *w* firms simultaneously upon arrival. While other types (i.e., non-zero) of hackers/threats attack only one firm upon arrival. We proposed two ways to model the loss cost associated with the software monoculture risk.

4.1: Firm independent or identical loss due to software monoculture risk

In this subsection, we are interested in analyzing the case where a type *s* hacker breaches a firm then it breaches all firms. We assume type *s* hacker uses some glitch/errors inherently associated with the commonly used software to breach the firm security process. Therefore, the breaching process is independent of the level of security implemented by the firm (i.e., breaching process for the commonly used software is the same for all firms). By hypothesis, we have

$\beta_s(m_k) \equiv P(Б_{kvs}(m_k,t)=1)=\beta_s$ and $Б_{kls}(t)=Б_{1ls}(t)$ for all t,k and l.
$Q_{ks}(t)=Q_{1s}(t)$; $B_{ks}(t)=B_{1s}(t)$; $R_{ks}(t)=R_{1s}(t)$ and $D_{ks}(t)=D_{1s}(t)$ for all *k* and *t.*

Let L_{kvs} denote the loss due to the v^{th}type *s* hacker breaches all counter measures of firm *k.* We assume that $\{L_{kvs}\equiv L_{vs}$; all k and $v\}$ are independent and identically distributed random variables with the first two moment of L_{kvs} as l_s *and* $l_s^{(2)}$(i.e., firm independent or identical loss). We let the random variable L_{kvi} $(i\neq s)$ denote the loss due to the v^{th}type *i* hacker breach all counter measures of firm *k.* We assume that $\{L_{kvi}$; all k,v and $i\neq s\}$ are independent and identically distributed random variables with the first two moment of L_{kvi} as l_{ki} *and* $l_{ki}^{(2)}$. In practice, we can utilize any available statistical methodologies that only uses the first two moments to estimate losses. For example, Lin et al 2022 reported that in an empirical study that gamma distribution is a good choice for estimating individual firm total loss due to cyber breach.

Utilizing equation (23), we can easily compute the mean and variance of $C_k(m_k,t)$ as

$$E\big(C_k(m_k,t)\big)=g_k(m_k)+E\big(B_{ks}(t)\big)l_s+\textstyle\sum_{i\in T_k\setminus\{s\}}E\big(B_{ki}(t)\big)\,l_{ki}. \quad (24)$$

$$Var\big(C_k(m_k,t)\big)=\Big[l_s^{(2)}-l_s^2\Big]E\big(B_{1s}(t)\big)+l_s^2Var\big(B_{1s}(t)\big) + \sum_{i\in T_k\setminus\{s\}}E\big(B_{ki}(t)\big)\Big[l_{ki}^{(2)}-l_{ki}^2\Big]+\sum_{i\in T_k\setminus\{s\}}Var\big(B_{ki}(t)\big)\,l_{ki}^2 \quad (25)$$

where one can find the formula for $E\big(B_{si}(t)\big)$; $E\big(B_{ki}(t)\big)$; $Var\big(B_{ki}(t)\big)$ and $Var\big(B_{1s}(t)\big)$ via theorem 2. Furthermore, we have for $k\neq j$; the covariance of firm's cost given by

$$Cov\Big(C_k(m_k,t),C_j\big(m_j,t\big)\Big)=Var\left(\textstyle\sum_{v=1}^{B_{1s}(t)}L_{vs}(t)\right)=\Big[l_s^{(2)}-l_s^2\Big]E\big(B_{1s}(t)\big)+l_s^2Var\big(B_{1s}(t)\big). \quad (26)$$

By hypothesis, there is no change in each firm *k* security investment (i.e., m_k) during the *t* periods planning horizon. Therefore, we have for all *k* and *j*

$$Cov\Big(C_k(m_k,t),C_j\big(m_j,h\big)\Big)=0 \text{ for } t\neq h. \quad (27)$$

The insurer pools the risk associated with its portfolio of *w* policyholders/firms. Risk pooling arrangements have two important effects. First, the variance or standard deviation of the average loss is reduced. Consequently, the probability of extreme outcomes for the firms participating in the risk pooling arrangement, both high and low, is reduced. Second, the distribution for the average loss becomes more bell-shaped (i.e., normal distribution) as the number of firms participating in the risk pool increases. We refer readers who are interested in learning more about insurance companies' risk pooling arrangement to Harrington and Niehaus (2004) which provide an excellent elementary introduction to the topic of risk pooling arrangements.

Notice that the *t*-periods risk faced by firm *k* is given by

$$\sum_{h=1}^{t}C_k(m_k,h). \quad (28)$$

The insurer pools the risk associated with its portfolio of *w* policyholders/firms. To implement the risk pooling arrangement, we define the *t*-periods average risk for the insurer, $\overline{C(t)}$ as

$$\overline{C(t)}=\left(\frac{1}{wt}\right)\sum_{h=1}^{t}\sum_{k=1}^{w}C_k(m_k,h). \quad (29)$$

Using equations (24)-(25), we can compute $E\big(\overline{C(t)}\big)$ and $Var\big(\overline{C(t)}\big)$

$$E(\overline{C(t)})=\left(\frac{1}{wt}\right)\sum_{h=1}^{t}\sum_{k=1}^{w}g_k(m_k,h)+E(B_{ks}(h))l_s+\sum_{i\in T_k\setminus\{s\}}E(B_{ki}(h))\,l_{ki} \text{ and} \quad (30)$$

$$Var\left(\overline{C(t)}\right) = \left(\frac{1}{wt}\right)^2 \sum_{h=1}^{t}[\sum_{k=1}^{w} Var\left(C_k(m_k,h)\right) + 2 \sum_{1\le j<k\le w} Cov\left(C_k(m_k,h), C_j(m_j,h)\right)]. \quad (31)$$

Notice that theorem 3 assures that the following long run mean and variance of the per period cost function for firm *k* exists and equals

$$E\left(C_k(m_k)\right) \equiv \lim_{t\to\infty} E(C_k(m_k),t) = g_k(m_k) + \frac{\beta_s(m_1)\lambda_{1s}}{1-r_{1s}} l_s + \sum_{i\in T_k\setminus\{s\}} \frac{\beta_i(m_k)\lambda_{ki}}{1-r_{ki}} l_{ki}; \quad (32)$$

$$Var\left(C_k(m_k)\right) \equiv \lim_{t\to\infty} Var(C_k(m_k),t) = l_s^{(2)} \frac{\beta_s(m_1)\lambda_{1s}}{1-r_{1s}} + \sum_{i\in T_k\setminus\{s\}} l_{ki}^{(2)} \frac{\beta_i(m_k)\lambda_{ki}}{1-r_{ki}}; \quad (33)$$

$$Cov\left(C_k(m_k), C_j(m_j)\right) \equiv \lim_{t\to\infty} Cov\left(C_k(m_k,t), C_j(m_j,t)\right) = l_s^{(2)} \frac{\beta_s(m_1)\lambda_{1s}}{1-r_{1s}} \quad \text{for } k \neq j. \quad (34)$$

Therefore, The Law of Large Numbers and theorem 3 assures that $\overline{C(t)}$ converges to the true average cost $\bar{C}$ as *t* get larger. Using theorem 3 and equations (32)-(34), we get

$$E(\bar{C}) = \left(\frac{1}{w}\right)\sum_{k=1}^{w}\{g_k(m_k) + \frac{\beta_s(m_k)\lambda_{ks}}{1-r_{ks}} l_s + \sum_{i\in T_k\setminus\{s\}} \frac{\beta_i(m_k)\lambda_{ki}}{1-r_{ki}} l_{ki}\} \text{ and} \quad (35)$$

$$Var(\bar{C}) = l_s^{(2)} \frac{\beta_s(m_1)\lambda_{1s}}{1-r_{1s}} + \left(\frac{1}{w}\right)^2 \sum_{k=1}^{w} \sum_{i\in T_k\setminus\{s\}} l_{ki}^{(2)} \frac{\beta_i(m_k)\lambda_{ki}}{1-r_{ki}}. \quad (36)$$

If the number of firms *w* is sufficiently large, the Lindeberg–Feller version of the Central Limit Theorem (Chow and Teicher 1997) applies and the distribution of $\bar{C}$ is approximately normal. Therefore, $\bar{C}$ can be approximated by a normal random variable with mean $E(\bar{C})$ and variance $V(\bar{C})$; $\bar{C}\sim N\left(E(\bar{C}), V(\bar{C})\right)$.

Furthermore, we have $0 < \lim_{w\to\infty} Var(\bar{C}) = l_s^{(2)} \frac{\beta_s(m_1)\lambda_{1s}}{1-r_{1s}} < Var\left(C_k(m_k)\right) for\ all\ k.$

Noticed that $\lim_{w\to\infty} Var(\bar{C}) > 0$ implies that type *s* hackers or software monoculture created positively correlated risk for all firms. Therefore, we see that pooling the risk within the insurer's portfolio cannot diversify away the software monoculture risk. However, pooling the risk within the insurer's portfolio does reduce risk for each firm.

Remark 6: (Independent risks) For the case of independent risks (i.e., equation (1)), we don't have special types of hackers that simultaneously attack all firms. Equation (35) remains the same, but equation (36) simplifies to

$$Var(\bar{C}) = \left(\frac{1}{w}\right)^2 Var(\sum_{k=1}^{w} C_k(m_k)) = \left(\frac{1}{w}\right)^2 \sum_{k=1}^{w} \sum_{i\in T_k} \frac{\beta_i(m_k)\lambda_{ki}}{1-r_{ki}} l_{ki}^{(2)}.$$

Let V^{ind} denote the variance obtained from the above equation and let V^{corr} denote the variance obtained from equation (36). With these notations, we have the impact of correlated risks given by

$$V^{corr} - V^{ind} = l_s^{(2)} \frac{\beta_s(m_1)\lambda_{1s}}{1-r_{1s}} (\frac{w-1}{w}) > 0.$$

Therefore, we see that correlated risk increases the variability of the cost incurred.

The case of identical firms.

An important special case is that all firms share the same risk profile. Then equations (35)-(36), reduce to

$$E(\bar{C}) = E\left(C_1(m_1)\right) = g_1(m_1) + \frac{\beta_s(m_1)\lambda_{1s}}{1-r_{1s}} l_{1s} + \sum_{i\in T_k\setminus\{s\}} \frac{\beta_i(m_1)\lambda_{1i}}{1-r_{1i}} l_{1i} \quad \text{and} \quad (37)$$

$$Var(\bar{C}) = l_s^{(2)} \frac{\beta_s(m_1)\lambda_{1s}}{1-r_{1s}} + \left(\frac{1}{w}\right)\sum_{i\in T_k\setminus\{s\}} l_{ki}^{(2)} \frac{\beta_i(m_k)\lambda_{ki}}{1-r_{ki}}. \quad (38)$$

Furthermore, we have

$$Var\left(C_1(m_1)\right) - Var(\bar{C}) = \left(\frac{w-1}{w}\right)\sum_{i\in T_k\setminus\{s\}} l_{ki}^{(2)} \frac{\beta_i(m_k)\lambda_{ki}}{1-r_{ki}} > 0.$$

Noticed that $V\left(C_1(m_1)\right) - V(\bar{C})$ is independent of the effect of type *s* hacker or software monoculture risk. Therefore, pooling risk from identical firms does reduce risk for each firm even with the present of software monoculture risk. However, pooling risk does not diversify the monoculture risk.

4.2. Firm dependent loss due to software monoculture risk

In this section, we assume that the breaching process for the commonly used software depends on the level of security that the firm implemented (i.e., firm security level dependent breaching process). Effectively, we are modeling the case where a type *s* hacker breaches a firm *k* but it may not necessarily breaches other firms (i.e., $\beta_s(m_k) \equiv P(Б_{kvs}(m_k,t) = 1)$ is a function of k and s).

We let the random variable L_{kvi} denote the loss due to the v^{th}type *i* hacker breach all counter measures of firm *k*. We assume that $\{L_{kvi}; \text{all } k \text{ and } v\}$ are independent and identically distributed random variables with the first two moment of L_{kvi} as l_{ki} *and* $l_{ki}^{(2)}$. Next, we can denote the period cost function for firm *k;* $C_k(m_k,t)$ as

$$C_k(m_k,t) = g_k(m_k) + \sum_{v=1}^{B_{ks}(t)} L_{kvs}(t) + \sum_{i\in T_k\setminus\{s\}} \sum_{v=1}^{B_{ki}(t)} L_{kvi}(t). \quad (39)$$

Therefore, we can compute the mean and variance of $C_k(m,t)$ as

$$E(C_k(m_k,t)) = g_k(m_k) + E(B_{ks}(t))l_{ks} + \textstyle\sum_{i\in T_k\setminus\{s\}} E(B_{ki}(t))\, l_{ki}. \quad (40)$$

$$Var\big(C_k(m_k,t)\big) = \left[l_{ks}^{(2)} - l_{ks}^2\right] E\big(B_{ks}(t)\big) + l_{ks}^2 Var\big(B_{ks}(t)\big) + \sum_{i\in T_k\setminus\{s\}} E\big(B_{ki}(t)\big)\left[l_{ki}^{(2)} - l_{ki}^2\right] + \sum_{i\in T_k\setminus\{s\}} Var\big(B_{ki}(t)\big)\, l_{ki}^2 \quad (41)$$

where $E\big(B_{ki}(t)\big), E\big(B_{ks}(t)\big), Var\big(B_{ki}(t)\big)$ and $Var\big(B_{ks}(t)\big)$ are given by theorem 2.

Furthermore, we have for $k \neq j$; the covariance of firm's cost given by

$$Cov\left(C_k(m_k,t), C_j(m_j,t)\right) = l_{ks}l_{js}\beta_s(m_k)\beta_s(m_j)(r_{ks}r_{js})^{t-1} Cov\left(Q_{ks}(1), Q_{js}(1)\right) + l_{ks}l_{js}\beta_s(m_k)\beta_s(m_j)\lambda_s\left(\frac{1-(r_{ks}r_{js})^t}{1-r_{ks}r_{js}}\right). \quad (42)$$

Using equations (40)-(42), we can easily compute $E\big(\overline{C(t)}\big)$ and $Var\big(\overline{C(t)}\big)$. Notice that theorem 3 assures that the following long run mean, variance and covariance of the per period cost function for firm *k* exists and equals

$$E\big(C_k(m_k)\big) \equiv \lim_{t\to\infty} E(C_k(m_k),t) = g_k(m_k) + g_k(m_k) + \frac{\beta_s(m_1)\lambda_{1s}}{1-r_{1s}} l_s + \textstyle\sum_{i\in T_k\setminus\{s\}} \frac{\beta_i(m_k)\lambda_{ki}}{1-r_{ki}} l_{ki}; \quad (43)$$

$$Var\big(C_k(m_k)\big) \equiv \lim_{t\to\infty} Var(C_k(m_k),t) = l_{ks}^{(2)} \frac{\beta_s(m_1)\lambda_{1s}}{1-r_{1s}} + \textstyle\sum_{i\in T_k\setminus\{s\}} \frac{\beta_i(m_k)\lambda_{ki}}{1-r_{ki}} l_{ki}^{(2)}; \quad (44)$$

$$Cov\left(C_k(m_k), C_j(m_j)\right) \equiv \lim_{t\to\infty} Cov\left(C_k(m_k,t), C_j(m_j,t)\right) = l_{ks}l_{js}\frac{\lambda_{1s}\beta_s(m_k)\beta_s(m_j)}{1-r_{ks}r_{js}}. \quad (45)$$

Using equations theorem 3 and equations (43)-(45), we can compute the mean and variance of $\bar{C}$;

$$E(\bar{C}) = \left(\frac{1}{w}\right)\textstyle\sum_{k=1}^{w}\{g_k(m_k) + \frac{\beta_s(m_1)\lambda_{1s}}{1-r_{1s}} l_s + \sum_{i\in T_k\setminus\{s\}} \frac{\beta_i(m_k)\lambda_{ki}}{1-r_{ki}} l_{ki}\} \text{ and} \quad (46)$$

$$Var(\bar{C}) = \left(\frac{1}{w^2}\right)\left(\textstyle\sum_{i\in T_k} l_{1i}^{(2)} \frac{\beta_i(m_k)\lambda_{ki}}{1-r_{ki}}\right) + \left(\frac{1}{w}\right)^2 2\textstyle\sum_{1\le k<j\le w} l_{ks}l_{js}\frac{\lambda_{1s}\beta_s(m_k)\beta_s(m_j)}{1-r_{ks}r_{js}} \quad (47)$$

Noticed that

$$\lim_{w\to\infty} Var(\bar{C}) = \lim_{w\to\infty}\left(\frac{1}{w}\right)^2 2\textstyle\sum_{1\le k<j\le w} Cov\left(C_k(m_k), C_j(m_j)\right)$$

which may not be 0. This is the result of correlated risk represented by type *s* hackers.

Remark 7: Noticed that equations (46)-(47) are different from equations (35)-(36). This is due to the difference in the breaching process assumptions (i.e., $\beta_s(m_k)$).

Remark 8: (Independent risks) For the case of independent risks, equation (47) reduces to

$$V(\bar{C}) = \left(\frac{1}{w}\right)^2 V\left(\textstyle\sum_{k=1}^{w} C_k(m_k)\right) = \left(\frac{1}{w}\right)^2 \textstyle\sum_{k=1}^{w}\sum_{i\in T_k} \frac{\beta_i(m_k)\lambda_{ki}}{1-r_{ki}} l_{ki}^{(2)}.$$

Let V^{ind} denote the variance obtained from the above equation and let V^{corr} denote the variance obtained from equation (47). With these notations, we have the impact of correlated risks given by

$$V^{corr} - V^{ind} = \left(\frac{1}{w}\right)^2 2\sum_{1\le k<j\le w} l_{ks}l_{js}\frac{\lambda_{1s}\beta_s(m_k)\beta_s(m_j)}{1-r_{ks}r_{js}} > 0.$$

Therefore, we see that correlated risk increases the variability of the cost incurred.

The case of identical firms.
An important special case is that all firms share the same risk profile. Then equations (46)-(47), reduce to

$$E(\bar{C}) = E\big(C_1(m_1)\big) = g_1(m_1) + \frac{\beta_s(m_1)\lambda_{1s}}{1-r_{1s}} l_{1s} + \sum_{i\in T_k\setminus\{s\}} \frac{\beta_i(m_1)\lambda_{1i}}{1-r_{1i}} l_{1i} \quad \text{and} \tag{48}$$

$$Var(\bar{C}) = \left(\frac{1}{w}\right)\left\{\sum_{i\in T_1} \frac{\beta_i(m_1)\lambda_{1i}}{1-r_{1i}} l_{1i}^{(2)}\right\} + \left(\frac{w-1}{w}\right)\left\{l_{1s}^2(\beta_s(m_1))^2 \frac{\lambda_{1s}}{1-{r_{1s}}^2}\right\}. \tag{49}$$

Noticed that using equations (44), (49) and theorem 3, we get

$$\lim_{w\to\infty} Var(\bar{C}) = l_{1s}^2(\beta_s(m_1))^2 \frac{\lambda_{1s}}{1-{r_{1s}}^2} \quad \text{and}$$

$$Var\big(C_1(m_1)\big) - Var(\bar{C})$$
$$= \left(\frac{w-1}{w}\right) \sum_{i\in T_1\setminus\{s\}} \frac{l_{1i}^{(2)}\beta_i(m_1)\lambda_{1i}}{1-r_{1i}} + \left(\frac{w-1}{w}\right)\left[l_{1s}^{(2)} - \frac{{l_{1s}}^2\beta_s(m_1)}{1+r_{1s}}\right]\frac{\beta_s(m_1)\lambda_{1s}}{1-r_{1s}} > 0.$$

Therefore, pooling risk from identical firms does reduce risk for each firm even with the present of software monoculture risk.

Section 5: Optimal level of cyber security investment

The previous sections described our risk quantification process. It allows us to quantify the relationship between financial loss from cyberattack types and cyber breaching or defense probability. The output of the risk quantification process serves as input for our cyber security investment cost analysis. The cyber security investment cost analysis aims to provide financial justification to managers with quantification of trade-off between financial loss from cyber security breaches and cyber security investment cost. The goal of the cyber security investment cost analysis is to minimize the total cost of both financial loss from cyber security breaches and cyber security investment cost for targeted cyber security defense.

The analysis in section 3 motivates us to set the cyber security insurance premium as a function of an organization's investment in cyber security (i.e., measures to reduce its risk). We also prefer a constant per period premium over the *t* periods planning horizon as no customers like premium increases. We propose the following per period insurance premium formula for our *t* period planning horizon

$$p(\theta_\alpha, t) = E(\bar{C}(t)) + \theta_\alpha\sqrt{V\big(\overline{C(t)}\big)} = E\big(\overline{C(t)}\big)\left(1 + \frac{\theta_\alpha\sqrt{V(\bar{C}(t))}}{E(\bar{C}(t))}\right) \tag{50}$$

where θ_α represent the weight that measures our attitude towards risk and is an appropriate critical value for confidence level $1-\alpha$ of the normal distribution. One can also interpret $\frac{\theta_\alpha\sqrt{V(\overline{C(t)})}}{E(\overline{C(t)})}$ as the loading associated with the insurance contract. The rationale for this premium formula is that if the number of firms *w* is sufficiently large, the Lindeberg–Feller version of the Central Limit Theorem (Chow and Teicher 1997) applies and the distribution of $\overline{C(t)}$ is approximately normal. Therefore, we have

$$P\left(\overline{C(t)} \le E\big(\overline{C(t)}\big) + \theta_\alpha\sqrt{V\big(\overline{C(t)}\big)}\right) = P(Z \le \theta_\alpha) = 1-\alpha.$$

From equations (13)-(14), one sees that $E(\overline{C(t)})$ is a linear function of the breaching probability $\beta_j(m_k)$ and $Var(\overline{C(t)})$ is a quadratic function of the breaching probability $\beta_j(m_k)$. Therefore, $p(\theta_\alpha, t)$ is a function of $(m_1, m_2, \dots, m_w)$, the firm's implemented level of investment in cyber security.

Another justification for our pricing formula is comparative statics. Intuitively, we would expect that insurance prices would increase if the loss, number of hackers/attacks or breaching probabilities increases. To see this, we let $p^{FISBP}(\theta_\alpha, t)$ (respectively, $p^{FDSBP}(\theta_\alpha, t)$) denote the pricing formula obtain by assuming firm independent of security breaching process (respectively, firm dependent of security breaching process). That is, we obtain $p^{FISBP}(\theta_\alpha, t)$ using equations (35)-(36) and we get $p^{FDSBP}(\theta_\alpha, t)$ using equations (46)-(47). Then, for $\mathcal{T}\epsilon\{FISBP, FDSBP\}$; each *k* and *i* we have

$$\frac{\partial p^{\mathcal{T}}(\theta_\alpha,t)}{\partial \lambda_s}>0;\ \frac{\partial p^{\mathcal{T}}(\theta_\alpha,t)}{\partial \lambda_{ki}}>0;\ \frac{\partial p^{\mathcal{T}}(\theta_\alpha,t)}{\partial l_{ks}}>0;\ \frac{\partial p^{\mathcal{T}}(\theta_\alpha,t)}{\partial l_{ki}}>0;$$
$$\frac{\partial p^{\mathcal{T}}(\theta_\alpha,t)}{\partial l_{ki}^{(2)}}>0;\ \frac{\partial p^{\mathcal{T}}(\theta_\alpha,t)}{\partial l_{ks}^{(2)}}>0;\ \frac{\partial p^{\mathcal{T}}(\theta_\alpha,t)}{\partial r_{ki}}>0;\frac{\partial p^{\mathcal{T}}(\theta_\alpha,t)}{\partial \beta_s(m_k)}>0;\ \frac{\partial p^{\mathcal{T}}(\theta_\alpha,t)}{\partial \beta_i(m_k)}>0.$$

The above comparative static results justify our intuition where $p^{FISBP}(\theta_\alpha,t)$ and $p^{FDSBP}(\theta_\alpha,t)$ are increasing function of number of hackers/attacks, breaching probabilities, retrial probabilities and the first two moments of loss. It also provides justification for the insurer to offer premium discount if the firm actively engages in reducing these sources of risks.

Next, we shall present our analysis of the multi-period optimal cybersecurity investment problem.

Mean-Standard Deviation approach to finding an Optimal level of cyber security investment.

We aim to find a set of counter measures which minimize the premium or cost incurred. Toward this goal, we formulate the following optimization problem **(OP)**

$$\min_{(m_1,m_2,\dots,m_w)} p(\theta_\alpha,t)=E\left(\overline{C(t)}\right)+\theta_\alpha\sqrt{V\left(\overline{C(t)}\right)}$$
$$s.t.\ 0\le m_k\le u\ \ for\ k=1,2,\dots,w$$

where u is the maximum level of security level available; θ_α represent the weight that measure our attitude towards risk and is an appropriate critical value for confidence level $1-\alpha$ of the normal distribution.

Thus, with probability $1-\alpha$ we are then assured that $\overline{C(t)}\le E(\bar{C}(t))+\theta_\alpha\sqrt{V\left(\overline{C(t)}\right)}$.

Therefore, it is reasonable to seek a level of security investment for all firms $(m_1,m_2,\dots,m_w)$ that minimizes this upper bound limit $p(\theta_\alpha,t)=E\left(\overline{C(t)}\right)+\theta_\alpha\sqrt{V\left(\overline{C(t)}\right)}$.

The solution of (OP) provides a guideline for the insurer to incentivize the individual firm to invest optimally in cyber security. For example, if the individual firm invests optimally in cyber security, then the insurer may lower the premium according to the solution of (OP). In general (OP) is a complicated nonlinear integer programming optimization problem. For example, the cybersecurity investment function $g_k(m)$ may not be convex and local optimal solution may not be global optimal solution for (OP). It is a well-known fact that integer programming and hence nonlinear integer programming is an NP-hard problem (i.e., there are no polynomial-time algorithmic solutions that exist for NP-hard problems). We refer the reader to (Li 2006) for an in-depth discussion on the difficulties and challenges for solving nonlinear integer programming.

Theorem 3 shows that our performance measures converge geometrically to their steady state values and the rate of convergence is given by r_{kj}. If ${r_{kj}}^t\approx 0$, then $p(\theta_\alpha)=E(\bar{C})+\theta_\alpha\sqrt{V(\bar{C})}\approx p(\theta_\alpha,t)$. Thus, the solution of (OP) can be approximated by the solution of the steady state version of the optimal pricing problem **(OP-I)**

$$\min_{(m_1,m_2,\dots,m_w)} p(\theta_\alpha)=E(\bar{C})+\theta_\alpha\sqrt{V(\bar{C})}$$
$$s.t.\ 0\le m_k\le u\ \ for\ k=1,2,\dots,w.$$

Lemma 1: Let $m^*(\theta)$ denote the optimal solution to (OP-I) as a function of θ. Then we have

$$m^*(\theta)\ge m^*(0).$$

Lemma 1 implies that mean value analysis (i.e., $\theta=0$) tend to underestimate the investment in cyber security level. This result confirms our intuition that mean analysis ignores the variability of loss cost and hence underestimated the level of cyber security investment. For the special case of mean analysis (i.e., $\theta=0$), (OP-I) simplifies substantially. Effectively, for mean value analysis, (OP-I) a w variables optimization problem reduces to w individual firm optimization problem with a single variable, the firm's cyber security investment level.

Lemma 2. Suppose that $\theta=0$. Let $m_i^*(t)$ be the solution to the following optimization problem

$$\min_{0\le m\le u} E(C_i(m,t))$$

and let m_i^* be the solution to the following optimization problem

$$\min_{0\le m\le u} E(C_i(m)).$$

Then, $(m_1^*(t), m_2^*(t), \dots, m_w^*(t))$ is the optimal solution for (OP) and $(m_1^*, m_2^*, \dots, m_w^*)$ is the optimal solution for (OP-I).

Lemma 3: For (OP-I), the optimal value for the case of firm independent loss due to software monoculture risk is larger than the optimal value for the case of firm dependent loss due to software monoculture risk.

Lemma 3 confirms our intuition that correlated risk imposes more loss cost than independent risk. We propose to examine numerically a variety of cases aimed at understanding the impact of cyber security investment versus average cost behavior. These numerical results also allow us to analyze the impact of correlated risk on the optimal level of cyber security investment for each firm.

Numerical results – identical suppliers

In this subsection, we shall perform some sensitivity analysis on numerical results obtained from solving (**OP-I**). We started out with a base case. Then we change the value of one of the parameters while keeping the value of *all* the other parameters at the base value. This allows us to isolate/highlight the individual effects of the variable under study and provides us with a guideline on how to choose the appropriate parameter value in setting up our pricing formula. To do that, we assume the case of identical firms and having the following parameters value as our base case:

$T = T_k = \{0,1,2,3\}; n_1 = n_k = 3; |T_k| = n_k + 1 = 4;$ *w=30; u=70;* $a = 0; \lambda_s = 156; \lambda_0 = \lambda_i = 104;$
$g_k(m) = 5m + 10m^2; l_s = 75; l_s^{(2)} = 2 * {l_{1s}}^2 = 11250; l_0 = l_{ki} = 50; l_0^{(2)} = l_{ki}^{(2)} = 2 * {l_0}^2 = 5000;$
$\beta_s = 0.25; \beta_s(m) = (0.25)^{m+1}; \beta_0(m) = \beta_i(m) = (0.8)^{m+1}; r_{ks} = 0.5(1-\beta_s); r_{ki} = 0.5\big(1-\beta_i(m)\big).$

When one of the parameter's values is changed, it is assumed that *all* the other parameters stay at the base value, unless otherwise noted. Tables 1–6 compare the numerical results given by (**OP-I)**. Each entry in the table represents an ordered pair. The first (respectively, second) entry of each order pair provides value of optimal security investment level for *FISBP* (respectively, *FDSBP*). For each of these ten tables, we tabulate the value of optimal level security investment with three values of $\theta_\alpha = 0, 1.645$ & 1.96. The case $\theta_\alpha = 0$ represents mean value analysis.

Table 1 consider sensitivity analysis when the value of $\beta_s$changes. Table 2 consider sensitivity analysis when the value of β_0 changes. Table 3 consider sensitivity analysis when the value of l_0 changes. Table 4 consider sensitivity analysis when the value of $g_1(m)$ changes. Table 5 consider sensitivity analysis when the value of λ_0 changes. Table 6 consider sensitivity analysis when the value of r_{11} changes.

Table 1 Optimal *m*: sensitivity analysis of the value of β_s

β_s (FISBP,FDSBP)			
β_s	$\theta_\alpha = 0$	$\theta_\alpha = 1.645$	$\theta_\alpha = 1.96$
0.01	(12,12)	(12,12)	(12,12)
0.05	(12,12)	(12,12)	(12,12)
0.1	(12,12)	(12,12)	(12,12)
0.25	(12,12)	(12,12)	(12,12)
0.4	(12,12)	(12,12)	(12,12)
0.5	(12,12)	(12,12)	(12,12)
0.65	(12,12)	(12,12)	(12,12)
0.8	(12,14)	(12,14)	(12,14)
0.95	(12,16)	(12,17)	(12,17)
0.99	(12,13)	(12,13)	(12,13)

Table 2 Optimal *m*: sensitivity analysis of the value of β_0			
β_0 (FISBP,FDSBP)			
β_0	$\theta_\alpha = 0$	$\theta_\alpha = 1.645$	$\theta_\alpha = 1.96$
0.01	(1,3)	(1,3)	(1,3)
0.05	(2,3)	(2,3)	(2,3)
0.1	(2,3)	(2,3)	(2,3)
0.25	(3,4)	(3,4)	(3,4)
0.4	(5,5)	(5,5)	(5,5)
0.5	(6,6)	(6,6)	(6,6)
0.65	(8,8)	(8,8)	(8,8)
0.8	(12,12)	(12,12)	(12,12)
0.95	(16,16)	(17,17)	(17,17)
0.99	(7,7)	(7,7)	(7,7)

The results given in Table 1 indicating that optimal value of m is not sensitive to changes in β_s. This is due to the fact that the nature of our optimization problem choose the optimal m to keep the number of breaches small. The number of breaches depends on both β_s (represent type *s* hacker) and β_0 (represent 4 types of hackers for this example). The value of β_0 remains the same even though the value of β_s changes. Therefore, the base case value of β_0 limit the changes in m. On the other hand, Table 2 indicates that the optimal value of m is more sensitive to changes in β_0 as β_0 is more impactful than β_s in keeping the number of breaches small.

Tables 1-2 indicate that FISBP tends to have lower optimal value of m as compared to FDSBP. This is consistent with lemma 3. As β_s *or* β_0 increases, the optimal level of investment in cyber security is increasing as θ_α increases. It is interesting to note that very high value of $\beta_0 = 0.99$ illustrate the case where increases investment in cyber security is not justified as the reduction in losses due to security investment is not as great as the investment needed to secure such reduction.

Table 3 Optimal *m*: sensitivity analysis of the value of l_0			
l_0 (FISBP,FDSBP) $\{l_0{}^{(2)} = 2(l_0)^2\}$			
l_0	$\theta_\alpha = 0$	$\theta_\alpha = 1.645$	$\theta_\alpha = 1.96$
50	(12,12)	(12,12)	(12,12)
150	(15,15)	(15,15)	(15,16)
300	(18,18)	(18,18)	(18,18)
600	(20,20)	(20,21)	(20,21)
1500	(24,24)	(24,24)	(24,24)
3000	(26,26)	(27,27)	(27,27)
6000	(29,29)	(30,30)	(30,30)
10000	(31,31)	(32,32)	(32,33)
15000	(33,33)	(34,34)	(34,35)
20000	(34,34)	(36,36)	(36,36)

Given that our base case value for $\beta_0 = 0.8$; tables 3 indicate that average loss $l_0$has a significant impact on optimal m. Rising average losses l_0 leads to higher level of m, investment in security.

Table 4 Optimal *m*: sensitivity analysis of the value of $g(m)$			
$g(m) = 5m + 10m^2$ (FISBP,FDSBP)			
$g(m)$=base	$\theta_\alpha = 0$	$\theta_\alpha = 1.645$	$\theta_\alpha = 1.96$
0.1*base	(20,20)	(20,20)	(20,20)
0.5*base	(14,14)	(14,14)	(14,14)
base	(12,12)	(12,12)	(12,12)
2*base	(9,9)	(9,9)	(9,9)
4*base	(7,7)	(7,7)	(7,7)
10*base	(5,5)	(5,5)	(5,5)
15*base	(4,4)	(4,4)	(4,4)

20*base	(3,3)	(3,4)	(3,4)
40*base	(2,2)	(2,2)	(2,2)
80*base	(1,2)	(1,2)	(1,2)

The numerical results in table 4 confirm our intuition that low investment cost leads to a higher level of security investment as it is cheap to do so. The converse is also true. High investment costs lead to a lower level of security investment as it is expensive to do so.

Table 5 Optimal *m*: sensitivity analysis of the value of λ_0			
λ_0 (FISBP,FDSBP)			
λ_0	$\theta_\alpha = 0$	$\theta_\alpha = 1.645$	$\theta_\alpha = 1.96$
52	(9,9)	(9,9)	(9,9)
104	(12,12)	(12,12)	(12,12)
156	(13,13)	(13,13)	(13,13)
208	(14,14)	(14,14)	(14,14)
260	(15,15)	(15,15)	(15,15)
312	(15,15)	(15,15)	(15,15)
364	(16,16)	(16,16)	(16,16)

With our base case value for $\beta_0 = 0.8$; table 5 indicate that average hacker arrival rate λ_0 has larger impact on optimal m. Rising average hacker arrival rate λ_0 means higher number of attacks and hence more breaches as our individual level breach probability of 0.8 is not low. Thus, to reduce the number of breaches the optimal level of security investment would need to increase.

Table 6 Optimal *m*: sensitivity analysis of the value of r_{11}			
r_{11} (FISBP,FDSBP)			
r_{11}=base	$\theta_\alpha = 0$	$\theta_\alpha = 1.645$	$\theta_\alpha = 1.96$
0	(11,11)	(11,11)	(11,11)
0.1*base	(11,11)	(11,11)	(11,11)
0.25*base	(11,11)	(11,11)	(11,11)
0.5*base	(11,11)	(11,12)	(11,12)
0.75*base	(11,11)	(11,12)	(11,12)
base	(12,12)	(12,12)	(12,12)
1.25*base	(12,12)	(12,12)	(12,12)
1.5*base	(12,12)	(12,12)	(12,12)
1.75*base	(12,12)	(12,12)	(12,12)
1.9*base	(12,12)	(12,12)	(12,12)

The results given in Table 6 indicates that the optimal value of m is more sensitive to changes in r_{11} as r_{11} is more impactful than r_{1s} in keeping the mean and variance of the number of breaches small. Furthermore, as r_{11} increases, the optimal level of investment in cyber security is nondecreasing as θ_α increases.

6. Conclusion

We develop a multiple-period/discrete-time stochastic cyber security breach model to study the effectiveness of our model in adjusting to potential future threats. Our model allows us to consider the transient effects of our discrete-time stochastic cyber security breaching model. It also allows us to model the possibility that a hacker who failed to breach the system in a period may decide to try breaching the system again in the next period. Our analysis allows us to take into consideration two types of breaching (identical across different firms and dependent on security implemented by the firm) process due to the software monoculture risk. We derive the mean, variance and covariance for the number of breaches for multiple types of hackers. Another significant difference between our approaches is that we derived our results as a byproduct of our model without assuming a particular form of security breach probability function. Furthermore, our approach shed light on how a firm could use cyber insurance in a multiple period planning horizon to manage its cyber security investment based on different characteristics of threat

environments and cyber security system configurations. To develop the cyber insurance pricing model, our method only requires us to know the first two moments of the loss associated with the firm. This flexibility allows us to utilize any available statistical methodologies that only uses the first two moments to estimate losses (e.g., Lin et al 2022). We proposed a mean-standard deviation approach to determine the optimal level of cyber security investment in the presence of multiple sources of risks. Our formulation of the problem generalizes the conventional mean value (or risk neutral) analysis. It also allows us to take into consideration the need to balance two conflicting objectives: loss and cyber security investment. Furthermore, it incentivizes the firm to engage in appropriate cyber security investment to reduce risk by providing premium discount that is a function of the firm's cyber security investment. Some theoretical results regarding the solution of the cyber security optimal investment problem are given. The comparative statics analysis given for our pricing formula indicates that it is an increasing function of number of hackers/attacks, breaching probabilities, retrial probabilities, and the first two moments of loss. We show that firms that engage in mean value analysis consistently underestimated the optimal cyber security investment. The numerical results are tabulated in Tables 1–6.

There are a few important and interesting open questions requiring more detailed analysis. The cost of cybersecurity insurance is based in part on cyber security investment, frequency, severity or loss due to cyber-attacks. It is a fact that cyber threats are continuously evolving and hence potential future threats also plays a role in determining cybersecurity insurance premium. To break away from escalating attacks and successfully deal with threat actors, there is a need to embrace a cyber security strategy that is constantly vigilant, actionably comprehensible, and adaptable to new threats or disruptive technologies.

One important research issue to consider is the *nonstationary* transient effects of our cyber security breaching model. For example, we may face a situation where there are 6 types of threats at the beginning of the year, and two new types of threats start emerging 9 months later. Therefore, it is important to develop the extension of our cybersecurity breaching model to capture the impact of the newly emerging threats or disruption technologies. Furthermore, our analysis takes the number of hackers/attacks as an exogeneous variable. It is worthwhile exploring the trade-off of investing in procedures that may reduce the number of hackers/attacks and the cost of implementing such deterrence across firms. One may frame this as an issue where firms in private industry find it in their interest to join forces, pool resources or forming associations to fight cyber-crime. In particular, we intend to explore the plausibility of examining numerically a variety of cases aimed at understanding the loss due to cyber-attacks vs. total cost behavior. These numerical results should give us some insights regarding our pricing model on the impact of risk and uncertainty in determining the appropriate cyber security insurance premium for the insurer and the optimal level of cyber security investment for the firms. We plan to extend our model toward analyzing such issues.

References

Australia regulator sues FIIG Securities for cybersecurity failures, March 13, 2025, Reuters.

Aven, T. Quantitative Risk Assessment: The Scientific Platform. Cambridge: Cambridge University Press, 2011.

Aven, T.; and Flage, R. Foundational challenges for advancing the field and discipline of risk analysis. Risk Analysis 40: 2128–36, 2020.

Callegaro, G.; Fontana, C.; Hillairet, C.; Ongarato, B. A stochastic Gordon-Loeb model for optimal cybersecurity investment under clustered attacks; Papers 2505.01221, arXiv.org **2025**.

Chong, Wing Fung, Feng, Runhuan , Hu, Hins, and Zhang, Linfeng. Cyber Risk Assessment for Capital Management. arXiv 2022. https://doi.org/10.48550/arXiv.2205.08435.

Chow, Y.S.; Teicher, H. Probability theory: independence, interchangeability, martingales. New York (NY): Springer; 1997.

CrowdStrike deploys fix for issue causing global tech outage. July 19, 2024, Reuters.

David, D.; Keupp, M.; Ghernaouti, S. and Mermoud, A.; Cyber-Security Investment in the Context of Disruptive Technologies-Extension of the Gordon-Loeb Model and Application to Critical Infrastructure Protection, 296-301, Critical Information Infrastructures Security; 11th International Conference, CRITIS 2016; Paris, France, October 10–12, 2016, Revised Selected Papers; Grigore Havarneanu; Roberto Setola; Hypatia Nassopoulos; Stephen Wolthusen (Eds.), Lecture Notes in Computer Science, Springer, 2018.

Franke, U. The cyber insurance market in Sweden. Computers & Security 68: 130–44, 2017.

Gordon, L.A.; Loeb, M.P. The economics of information security investment. ACM Trans. Inf. Syst. Secur. 2002, 5, 438–457.

Gordon, L.A.; Loeb, M.P.; Zhou, L. Investing in Cybersecurity: Insights from the Gordon-Loeb Model. J. Inf. Secur. 2016, 7, 49.

Gordon, L.A.; Loeb, M.P.; Lucyshyn, W.; Zhou, L. Increasing cybersecurity investments in private sector firms. J. Cybersecur. 2015, 1, 3–17.

Harrington, S. and Niehaus, G. Risk Management and Insurance, (2nd ed.). Boston, MA, Irwin; 2004.

Hausken, K. Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. Inf. Syst. Front. 2006, 8, 338–349.

Heiding, F.; Schneier, B.; Vishwanath, A. AI Will Increase the Quantity — and Quality — of Phishing Scams; Harvard Business Review 30-5-2024.

Huang,D.; Hu,Q.; Behara, R. An economic analysis of the optimal information security investment in the case of a risk-averse firm. Int. J. Prod. Econ. 2008, 114, 793–804.

IBM. Cost of a Data Breach Report 2023, 2023.

Khalili, M., Naghizadeh, P., Liu, M. Designing cyber insurance policies: The role of pre-screening and security interdependence. IEEE Transactions on Information Forensics and Security 13: 2226–39, 2018.

Krutilla, K.; Alexeev, A.; Jardine, E.; Good, D. The Benefits and Costs of Cybersecurity Risk Reduction: A Dynamic Extension of the Gordon and Loeb Model. Risk Anal. 41, 1795–1808, 2021.

Lee, Y.S. Thomas. Integrated Cyber Security Risk Management-Insurance and Investment Cost Analysis. International Journal of Data Analysis Techniques and Strategies, Vol. 16, No. 3, 223-261, 2024.

Li, D.; Sun, X. Nonlinear Integer Programming. New York (NY): Springer; 2006.

Lin, Z., Sapp, T., Parsa, R., Ulmer, J., Cao, C. Pricing Cyber Security Insurance, Journal of Mathematical Finance, 12, 46-70, 2022.

Marotta, A., Martinelli, F., Nanni, S., Orlando, A., Yautsiukhin, A. Cyber-insurance survey. Computer Science Review 24, 35–61, 2017.

Mastroeni, L., Mazzoccoli, A., Naldi, M. Service level agreement violations in cloud storage: Insurance and compensation sustainability. Future Internet 11: 142, 2019.

Mazzoccoli, A. Optimal Cyber Security Investment in a Mixed Risk Management Framework: Examining the Role of Cyber Insurance and Expenditure Analysis, Risks, Vol. 11, Issue 9, 154, 2023.

Mazzoccoli, A.; Naldi, M. Robustness of optimal investment decisions in mixed insurance/investment cyber risk management. Risks Analysis, 40, 550-564, 2020a.

Mazzoccoli, A.; Naldi, M. The expected utility insurance premium principle with fourth-order statistics: Does it make a difference? Algorithms 13: 116, 2020b.

Mazzoccoli, A.; Naldi, M. Optimal Investment in Cyber-Security under Cyber Insurance for a Multi-Branch Firm. Risks, 9, 24, 2021.

Mazzoccoli, A.; Naldi, M. Optimizing Cybersecurity Investments over Time. Algorithms, 15, 6, https://doi.org/10.3390/a15060211, 2022.

Mayadunne, S.; Park, S. An economic model to evaluate information security investment of risk-taking small and medium enterprises. Int. J. Prod. Econ. 182, 519–530, 2016.

Mukhopadhyay, A., Chatterjee, S., Bagchi, K., Kirs, P.; Shukla, G. Cyber risk assessment and mitigation (cram) framework using logit and probit models for cyber insurance. Information Systems Frontiers 21: 997–1018, 2019.

Naldi, M., Mazzoccoli, A. Computation of the insurance premium for cloud services based on fourth-order statistics. International Journal of Simulation: Systems, Science and Technology 19, 1–6, 2018.

Petrosyan, A. Cyber attacks: most common exploited applications worldwide 2021-2022, Statista, 2023. https://www.statista.com/statistics/434880/cyber-crime-common-exploits-global/

Ponemon, L. 2011 Cost of Data Breach Study: United States. Technical report, Ponemon Institute, 2011.

Rosson, J., Rice, M., Lopez, J., Fass, D. Incentivizing Cyber Security Investment in the Power Sector Using an Extended Cyber Insurance Framework. Homeland Security Affairs 15: 1–25, 2019.

Sobers, R. 84 Must-Know Data Breach Statistics, Varonis 2023.
https://www.varonis.com/blog/data-breach-statistics#:~:text=In%202023%2C%20the%20United%20States,million%20in%202021%20(IBM).

Strupczewski, G. Current state of the cyber insurance market. Paper presented at 10th Economics and Finance Conference, Rome, Italy, September 10–13, 2018. Number 6910062. Rome: International Institute of Social and Economic Sciences.

VIPRE's Email Threat Trends Report 2024, https://vipre.com/resources/email-threats-latest-trends-q2-2024.

Wang, S. Integrated framework for information security investment and cyber insurance. Pac.-Basin Financ. J. 2019, 57, 101173.

Wang, S. Optimal Level and Allocation of Cybersecurity Spending: Model and Formula. SSRN Electronic Journal, 2017.

Wang, S. Optimal Level and Allocation of Cybersecurity Spending, Risk Management, 16-18, March 2018.

Wu, Y.; Feng, G.; Wang, N.; Liang, H. Game of information security investment: Impact of attack types and network vulnerability. Expert Syst. Appl., 42, 6132–6146, 2015.

Xu, L.; Li, Y.; and Fu, J. Cybersecurity investment allocation for a multi-branch firm: Modeling and optimization. Mathematics 7, 587, 2019.

Young, D.; Lopez, J.; Rice, M.; Ramsey, B.; and McTasney, R. A framework for incorporating insurance in critical infrastructure cyber risk strategies. Int. J. Critical Infrastructure Protection, 182, 43–57, 2016.

Zhuo, Y.; Solak, S. Measuring and optimizing cybersecurity investments: A quantitative portfolio approach. In Proceedings of the IIE Annual Conference, Montreal, QC, Canada, 31 May–3 June 2014; p. 1620.

Appendix

Proof of Theorem 1: Recall the flow balance equation

$$Q_{ki}(t+1) = Q_{ki}(t) + A_{ki}(t) - D_{ki}(t) - B_{ki}(t) = R_{ki}(t). \quad (3)$$

Using equation (3) and (4), we get

$$E\left(Q_{kj}(t+1)\middle|Q_{kj}(t), A_{kj}(t)\right) = E\left(R_{kj}(t)\middle|Q_{kj}(t), A_{kj}(t)\right) = r_{kj}(Q_{kj}(t) + A_{kj}(t)).$$

Therefore, we get

$$E(Q_{kj}(t+1)) = r_{kj}(E(Q_{ki}(t)) + \lambda_{kj}) = r_{kj}E(Q_{ki}(t)) + r_{kj}\lambda_{kj}.$$

Now, equation (8) follows from repeated application of the above equation. Next, using the conditional variance formula, we get

$$Var(Q_{kj}(t+1)) = EVar\left(R_{kj}(t)\middle|Q_{kj}(t), A_{kj}(t)\right) + Var\big(E(R_{kj}(t)\big|Q_{kj}(t), A_{kj}(t))\big). \quad (51)$$

Using equation (4), we get

$$Var\left(R_{kj}(t)\middle|Q_{kj}(t), A_{kj}(t)\right) = r_{kj}(1 - r_{kj})\left(Q_{kj}(t) + A_{kj}(t)\right).$$

Therefore, we have

$$\begin{aligned} EVar\left(R_{kj}(t)\middle|Q_{kj}(t), A_{kj}(t)\right) &= r_{kj}(1 - r_{kj})\big(E(Q_{kj}(t)) + \lambda_{kj}\big) \\ &= r_{kj}(1 - r_{kj})E\left(Q_{kj}(t)\right) + r_{kj}(1 - r_{kj})\lambda_{kj}. \end{aligned} \quad (52)$$

Next, using equation (4), we get

$$Var\big(E(R_{kj}(t)\big|Q_{kj}(t), A_{kj}(t))\big) = Var(r_{kj}\left(Q_{kj}(t) + A_{kj}(t)\right) = {r_{kj}}^2 Var\left(Q_{kj}(t)\right) + {r_{kj}}^2\lambda_{kj}. \quad (53)$$

Thus, substituting equations (52) and (53) into equation (51), we get

$$Var(Q_{kj}(t+1)) = {r_{kj}}^2 Var\left(Q_{kj}(t)\right) + {r_{kj}}^2\lambda_{kj} += r_{kj}(1 - r_{kj})E\left(Q_{kj}(t)\right) + r_{kj}(1 - r_{kj})\lambda_{kj}.$$

Now, equation (9) follows from repeated application of the above equation. Lastly, notice that by hypothesis, we have that $A_{ks}(t) = A_{js}(t)$ for all k and j. Next using the conditional covariance formula, we get for $k \neq j$;

$$\begin{aligned} Cov\left(Q_{ks}(t+1), Q_{js}(t+1)\right) &= Cov\left(R_{ks}(t), R_{js}(t)\right) \\ &= E(Cov\left(R_{ks}(t), R_{js}(t)|Q_{ks}(t), Q_{js}(t), A_{ks}(t)\right) \\ &+ Cov\left(E(R_{ks}(t)|Q_{ks}(t), Q_{js}(t), A_{ks}(t)), E(R_{js}(t)|Q_{ks}(t), Q_{js}(t), A_{ks}(t)\right) \\ &= 0 + Cov\left(r_{kj}\big(Q_{ks}(t) + A_{ks}(t)\big), r_{kj}\left(Q_{js}(t) + A_{ks}(t)\right)\right) \\ &= r_{ks}r_{js}Cov\left(Q_{ks}(t), Q_{js}(t)\right) + r_{ks}r_{js}\lambda_s. \end{aligned}$$

Now, equation (10) follows easily from repeated application of the above equation. ■

Proof of Theorem 2: From the flow balance equation (3), we have $Q_{kj}(t+1) = R_{kj}(t)$. Therefore, equations (11)-(12) follow from equations (8)-(9). By hypothesis, we have

$$\begin{aligned} E\left(B_{kj}(t)\right) = E\left\{E\left(B_{kj}(t)\middle|Q_{kj}(t), A_{kj}(t)\right)\right\} &= E\left\{\beta_j(m_k)\left(Q_{kj}(t) + A_{kj}(t)\right)\right\} \\ &= \beta_j(m_k)E(Q_{ki}(t)) + \beta_j(m_k)\lambda_{kj}. \end{aligned}$$

Now, equation (13) follows from repeated application of the above equation. Next, using the conditional variance formula, we get

$$Var(B_{kj}(t+1)) = EVar\left(B_{kj}(t)\middle|Q_{kj}(t), A_{kj}(t)\right) + Var\big(E(B_{kj}(t)\big|Q_{kj}(t), A_{kj}(t))\big). \quad (54)$$

Using equation (4), we get

$$Var\left(B_{kj}(t)\middle|Q_{kj}(t), A_{kj}(t)\right) = \beta_j(m_k)\left(1 - \beta_j(m_k)\right)\left(Q_{kj}(t) + A_{kj}(t)\right). \quad (55)$$

Therefore, we have

$$\begin{aligned} EVar\left(B_{kj}(t)\middle|Q_{kj}(t), A_{kj}(t)\right) &= \beta_j(m_k)\left(1 - \beta_j(m_k)\right)\big(E(Q_{kj}(t)) + \lambda_{kj}\big) \\ &= \beta_j(m_k)\left(1 - \beta_j(m_k)\right)E\left(Q_{kj}(t)\right) + \beta_j(m_k)\left(1 - \beta_j(m_k)\right)\lambda_{kj}. \end{aligned} \quad (56)$$

Next, using equation (4) we have

$$\begin{aligned} Var\big(E(R_{kj}(t)\big|Q_{kj}(t), A_{kj}(t))\big) &= Var(\beta_j(m_k)\left(Q_{kj}(t) + A_{kj}(t)\right) \\ &= \beta_j(m_k)^2 Var\left(Q_{kj}(t)\right) + \beta_j(m_k)^2\lambda_{kj}. \end{aligned} \quad (57)$$

Thus, substituting equations (56) and (57) into equation (54), we get

$$Var(B_{kj}(t)) = \beta_j(m_k)^2 Var\left(Q_{kj}(t)\right) + \beta_j(m_k)^2\lambda_{kj} + \beta_j(m_k)\left(1-\beta_j(m_k)\right)E\left(Q_{kj}(t)\right) + \beta_j(m_k)\left(1-\beta_j(m_k)\right)\lambda_{kj}.$$

Now, equation (14) follows from repeated application of the above equation. The proof of equations (15)-(16) is identical to the proof of equations (13)-(14) and hence omitted. Lastly, using the conditional covariance formula, we get for $k \neq j$;

$$\begin{aligned} Cov\left(B_{ks}(t), B_{js}(t)\right) &= E(Cov\left(B_{ks}(t), B_{js}(t)|Q_{ks}(t), Q_{js}(t), A_{ks}(t)\right) \\ &\quad + Cov\left(E(B_{ks}(t)|Q_{ks}(t), Q_{js}(t), A_{ks}(t)), E(B_{js}(t)|Q_{ks}(t), Q_{js}(t), A_{ks}(t)\right) \\ &= 0 + Cov\left(\beta_s(m_k)\left(Q_{ks}(t)+A_{ks}(t)\right), \beta_s(m_k)\left(Q_{js}(t)+A_{ks}(t)\right)\right) \\ &= \beta_s(m_k)\beta_s(m_j)Cov\left(Q_{ks}(t), Q_{js}(t)\right) + \beta_s(m_k)\beta_s(m_j)\lambda_s \quad (58) \end{aligned}$$

where the first equality follows from the fact that given $Q_{ks}(t), Q_{js}(t), A_{ks}(t)$; $B_{ks}(t)$ and $B_{js}(t)$ are independent random variables. Now, equation (15) follows from substituting equation (10) into the above equation. ■

Proof of Theorem 3: By definition $0 \leq r_{kj}, \beta_j(m_k), d_{kj}$ and $r_{kj} + \beta_j(m_k) + d_{kj} = 1$ for all *k* and *j*. Thus, we have $\lim_{t\to\infty} {r_{kj}}^t = 0$; for all *k* and *j*. Now, Theorem 3 follows easily from Theorem 1 and 2 by taking limit as $t \to \infty$ of equations (8)-(17). ■

Proof of equation (42): We have for $k \neq j$; the covariance of firm's cost given by

$$\begin{aligned} Cov\left(C_k(m_k,t), C_j(m_j,t)\right) &= Cov\left(\sum_{v=1}^{B_{ks}(t)} L_{kvs}(t), \sum_{v=1}^{B_{js}(t)} L_{jvs}(t)\right) \\ &= E\left\{Cov\left(\sum_{v=1}^{B_{ks}(t)} L_{kvs}(t), \sum_{v=1}^{B_{js}(t)} L_{jvs}(t)\right)\middle| B_{ks}(t), B_{js}(t)\right\} \\ &\quad + Cov\left(E\left(\sum_{v=1}^{B_{ks}(t)} L_{kvs}(t)\middle| B_{ks}(t)\right), E\left(\sum_{v=1}^{B_{js}(t)} L_{jvs}(t)\middle| B_{js}(t)\right)\right) \\ &= 0 + Cov\left(l_{ks}B_{ks}(t), l_{js}B_{js}(t)\right) \\ &= l_{ks}l_{js}\beta_s(m_k)\beta_s(m_j)Cov\left(Q_{ks}(t), Q_{js}(t)\right) + l_{ks}l_{js}\beta_s(m_k)\beta_s(m_j)\lambda_s \\ &= l_{ks}l_{js}\beta_s(m_k)\beta_s(m_j)(r_{ks}r_{js})^{t-1}Cov\left(Q_{ks}(1), Q_{js}(1)\right) + l_{ks}l_{js}\beta_s(m_k)\beta_s(m_j)\lambda_s\left(\frac{1-(r_{ks}r_{js})^t}{1-r_{ks}r_{js}}\right) \end{aligned}$$

where the third equality follows from the fact that given $B_{ks}(t), B_{js}(t)$ and $k \neq j$; $\sum_{v=1}^{B_{ks}(t)} L_{kvs}(t)$ and $\sum_{v=1}^{B_{js}(t)} L_{jvs}(t)$ are independent random variables and the last equality follows from theorem 1. ■

Proof of Lemma 1: By definition, we have

$$E(\bar{C}(m^*(0))) \leq E\left(\bar{C}(m^*(\theta))\right) \text{ and} \quad (59)$$

$$E\left(\overline{C}(m^*(\theta))\right) + \theta\sqrt{V\left(\bar{C}(m^*(\theta))\right)} \leq E\left(\overline{C}(m^*(0))\right) + \theta\sqrt{V\left(\bar{C}(m^*(0))\right)} \quad (60)$$

Rearranging terms from equation (60);

$$\theta\sqrt{V\left(\bar{C}(m^*(0))\right)} \geq E\left(\overline{C}(m^*(\theta))\right) - E\left(\overline{C}(m^*(0))\right) + \theta\sqrt{V\left(\bar{C}(m^*(\theta))\right)} \geq \theta\sqrt{V\left(\bar{C}(m^*(\theta))\right)}.$$

where the last inequality follows from equation (59). Thus, we have

$$V\left(\bar{C}(m^*(\theta))\right) \leq V\left(\bar{C}(m^*(0))\right). \quad (61)$$

Noticed that equation (36) or (47) indicates that all the coefficients of the variance function are positive. By definition of $\beta_{ki}(.)$, we have for all *k*, *i* and *j*

$\beta_{ki}(m^*(0)) - \beta_{ki}(m^*(\theta)) \geq 0$ if and only if $m^*(\theta) \geq m^*(0)$ and

$\beta_{ki}(m^*(0)) - \beta_{ki}(m^*(\theta)) \geq 0$ if and only if $\beta_{kj}(m^*(0)) - \beta_{kj}(m^*(\theta)) \geq 0$.

Therefore, substituting equation (36) or (47) into equation (61), and using the above observations about $\beta_i(.)$, we conclude that $\beta_i\big(m^*(0)\big) - \beta_i(m^*(\theta)) \geq 0$ and hence $m^*(\theta) \geq m^*(0)$. ■

Proof of Lemma 2: The result follows easily by noticing that the objective functions $E(\bar{C}(t))$ *and* $E(\bar{C})$ are separable and

$$\bar{C}(t) = \left(\frac{1}{wt}\right)\sum_{h=1}^{t}\sum_{k=1}^{w} C_k(m_k, h) \text{ and } \bar{C} = \left(\frac{1}{w}\right)\sum_{k=1}^{w} C_k(m_k).$$

Thus, we have

$\min\limits_{0\leq m_i\leq u} E(\bar{C}(t)) = \left(\frac{1}{wt}\right)\sum_{k=1}^{w} \min\limits_{0\leq m_k\leq u} \sum_{h=1}^{t} E\big(C_k(m_k, h)\big)$ & $\min\limits_{0\leq m_i\leq u} E(\bar{C}) = \left(\frac{1}{w}\right)\sum_{i=1}^{w} \min\limits_{0\leq m_i\leq u} E\big(C_i(m_i)\big)$. ■

Proof of Lemma 3: For the case of firm independent loss due to software monoculture risk, we get from equations (35)-(36),

$$\hat{P}_{FIL}(\theta_\alpha, m) = E(\bar{C}) + \theta_\alpha\sqrt{V(\bar{C})} = \left(\frac{1}{w}\right)\sum_{k=1}^{w}\{g_k(m_k) + \frac{\beta_s(m_k)\lambda_{ks}}{1-r_{ks}} l_s + \sum_{i\in T_k\setminus\{s\}} \frac{\beta_i(m_k)\lambda_{ki}}{1-r_{ki}} l_{ki}\}$$
$$+ \theta_\alpha\sqrt{l_s^{(2)}\frac{\beta_s(m_1)\lambda_{1s}}{1-r_{1s}} + \left(\frac{1}{w}\right)^2 \sum_{k=1}^{w}\sum_{i\in T_k\setminus\{s\}} l_{ki}^{(2)}\frac{\beta_i(m_k)\lambda_{ki}}{1-r_{ki}}}\ . \quad (62)$$

For the case of firm dependent loss due to software monoculture risk, we get from equations (46)-(47),

$$\hat{P}_{FDL}(\theta_\alpha, m) = E(\bar{C}) + \theta_\alpha\sqrt{V(\bar{C})} = \left(\frac{1}{w}\right)\sum_{k=1}^{w}\{g_k(m_k) + \frac{\beta_s(m_k)\lambda_{ks}}{1-r_{ks}} l_s + \sum_{i\in T_k\setminus\{s\}} \frac{\beta_i(m_k)\lambda_{ki}}{1-r_{ki}} l_{ki}\}$$
$$+ \theta_\alpha\sqrt{\left(\frac{1}{w^2}\right)\left(\sum_{i\in T_k} l_{1i}^{(2)}\frac{\beta_i(m_k)\lambda_{ki}}{1-r_{ki}}\right) + \left(\frac{1}{w}\right)^2 2\sum_{1\leq k<j\leq w} l_{ks}l_{js}\frac{\lambda_{1s}\beta_s(m_k)\beta_s(m_j)}{1-r_{ks}r_{js}}}\ . \quad (63)$$

Let m^{FIL}denote the optimal solution of (OP I-I) with equation (62) as objective function. Let m^{FDL} denote the optimal solution of (OP I-I) with equation (63) as objective function. Then, we have

$$\hat{P}_{FDL}(\theta_\alpha, m^{FDL}) \leq \hat{P}_{FDL}(\theta_\alpha, m^{FIL}) \leq \hat{P}_{FIL}(\theta_\alpha, m^{FDL})$$

where the first inequality follows from the definition of m^{FDL} and the second inequality follows from the observation that $\beta_s \geq \beta_s(m)$ implies that we have $\hat{P}_{FIL}(\theta_\alpha, m) \geq \hat{P}_{FDL}(\theta_\alpha, m)$. ■.