Hindawi
Mathematical Problems in Engineering
Volume 2020, Article ID 3239591, 10 pages
https://doi.org/10.1155/2020/3239591

Research Article

Modeling the Effect of Spending on Cyber Security by Using Surplus Process

Ciyu Nie,[1] Jingchao Li,[2,3] and Shaun Wang[4]

[1]*Division of Banking and Finance, Nanyang Business School, Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798*
[2]*College of Mathematics and Statistics, Shenzhen University, Nanhai Ave 3688, Shenzhen, Guangdong 518060, China*
[3]*Shenzhen Key Laboratory of Advanced Machine Learning and Applications, Shenzhen University, Shenzhen, Guangdong 518060, China*
[4]*Department of Finance, Southern University of Science and Technology, 1088 Xueyuan Avenue, Shenzhen, Guangdong 518055, China*

Correspondence should be addressed to Jingchao Li; jingchaoli@szu.edu.cn

Received 1 May 2020; Accepted 8 June 2020; Published 7 July 2020

Guest Editor: Wenguang Yu

In this paper, we assume the security level of a system is a quantifiable metric and apply the insurance company ruin theory in assessing the defense failure frequencies. The current security level of an information system can be viewed as the initial insurer surplus; defense investment can be viewed as premium income resulting in an increase in the security level; cyberattack arrivals follow a Poisson process, and the impact of attacks is modeled as losses on the security level. The occurrence of cyber breach is modeled as a ruin event. We use this framework to determine optimal investment in cyber security that minimizes the total cyber costs. We show by numerical examples that there is an optimal allocation of total cyber security budget to (1) IT security maintenance/upkeep spending versus (2) external cyber risk transfer.

1. Introduction

Cyber risk has become a hot topic given the ever-increasing cyber breaches and resulting losses of data and business disruptions. Cyber risk differs from traditional insurance risks in that they are very much driven by human behaviours in terms of attacks and defenses. What quantitative tools can actuaries imply to offer insights in measuring and managing cyber risks? In this paper, we apply traditional ruin theory in an innovative way to assess the stochastic changes in the level of cyber security and derived interesting insights from this theoretical framework.

Traditional actuarial ruin theory was developed in modeling of insurance capital solvency, whereas the level of capital is influenced by two opposing forces: the upward drift driven by a stream of insurance premium income and the random downward jump driven by insurance claims. During our literature review for cyber risk analysis (mostly from the computer science literature), we noticed that in many of the quantitative models, the security level of a system could be assumed as a quantifiable amount, which is primarily affected by the amount of investment in security development. In addition, it is commonly assumed that the probability and the loss severity of a defense failure (a cyber breach) depend on the security development and the damage control scheme.

In this paper, we assume the security level of a system is a quantifiable metric and apply the ruin theoretic framework in assessing the defense failure frequencies. We assume that the security level of a system changes over time due to attack and defense. The security level is then modeled by a modified surplus process: the current security level of an information system can be viewed as the initial surplus; defense investment resulting in an increase in the security level can be viewed as the premium income; the cyberattack arrivals are modeled as a Poisson process, and the impact of attacks is modeled as losses on the security level using an assumed loss

distribution. A cyberattack succeeds (or the defense fails) when ruin occurs. In other words, we apply the risk process to model the frequency of the cyber failure. Once the defense failed, an independent financial loss amount is incurred depending on the nature of data being breached. Our goal of this paper is to provide a framework for analyzing the economical relationship between IT security investment and the associated cyber breach losses and to use this framework to make optimal IT security investment decisions.

In Section 2, we provide a detailed description of the model. We then derive the formula for the distribution of defense failure frequency, which is a function depending on security investments and attack arrivals. Assuming the distribution of the loss severity from a cyber breach is known, we show that the optimal investment amount can be solved by minimizing the expected total cyber costs. In Section 3, we use numerical calculations to provide insights on the changes in expected total cyber costs and the optimal amount of cyber investment, under different assumptions of loss severity, attack arrival as well as time horizon. We also provide a literature review on cyber risk modeling in Section 4 and comment on future research in Section 5.

To our knowledge, this paper is the first attempt to model cyber risk by applying the ruin theory in the literature. The goal of this paper is not to propose a new actuarial model for cyber losses (in terms of frequency and severity distributions), but instead, we apply the ruin theoretical framework to the level of cyber security over the course of time, under opposing forces of attackers and defenders. We then use the framework to draw insights about optimal allocation of cyber security budget.

2. Surplus Process for the Cyber Security Level over Time

2.1. Surplus Processes in the Classical Ruin Theory. We first review the classical insurance surplus process defined by

$$U_t = u + ct - \sum_{i=1}^{N_t} X_i, \tag{1}$$

where $u = U_0$ is the initial surplus, c is a constant rate of premium income per unit time, $\{N_t\}_{t\geq 0}$ is a counting process for the number of claims, and $\{X_i\}_{i=1}^{\infty}$ is a sequence of i.i.d. random variables representing individual claim amounts with probability density function (p.d.f.) $f(x)$ and cumulative distribution function (c.d.f.) $F(x)$. Let T_u be the time that surplus first falls below 0 given initial surplus u, and the ultimate ruin probability is defined as $\psi(u) = \Pr(T_u < \infty)$. Under the classical risk model, it is common to assume $ct > E(\sum_{i=1}^{N_t} X_i)$ to ensure $\psi(u)$ is not 1. Define $\omega_u(t)$ to be the defective density function of T_u and $\widetilde{\omega}_u(s) = \int_0^{\infty} e^{-st}\omega_u(t)\mathrm{d}t, s \geq 0$, as the Laplace transform of $\omega_u(t)$. The conditional density of $T_u | T_u < \infty$ is denoted as $\omega_u^c(t) = \omega_u(t)/\psi(u)$.

2.2. Cyber Security Level Model Description. Gordon and Loeb [1] defined a vulnerability term ν, as the probability that an attack being successful. The observation is that the vulnerability of a security system is not static over time and it depends on the maintenance effort of the system administrator through time.

Denote ν_t as the vulnerability level of a security system at time t. In addition, we define the strength level of a security system at time t as u_t, where $\nu_t = g(u_t)$ and $g(x) \in [0,1], x \geq 0$, is a function that satisfies the following properties:

(1) $g'(x) < 0$, i.e., the higher the u_t is, the lower the vulnerability of the security system.

(2) When $x = 0$, $g(x) = 0$, i.e., when the strength level is 0, the probability of an attack being successful is 1.

(3) When $x \to \infty$, $g(x) \to 0$, i.e., when the strength level is extremely high, the probability of an attack being successful tends to 0. Here we assume that the security system cannot be completely protected; however, the system administrator manages it. There is always a probability of being breached.

One type of function that satisfies the above properties is where $g(x) = e^{-\alpha x}$, i.e., $\nu_t = e^{-\alpha u_t}$, where α is a parameter that transforms the strength level measurement u_t to a probability measurement ν_t.

We now apply some of the surplus process ideas to model the security strength level process of a firm's information system. Assume that process $\{u_t\}_{t\geq 0}$ represents the security strength at any time $t \geq 0$ of the system and that u_0 represents the system's current security level.

Let $\xi_t \geq 0$ denote the monetary (e.g., dollar) investment in security to protect the system. The result of such investment will create changes in security strength level u_t over time. For simplicity in our model, we assume that the investment is constant at ξ per unit of time and that the change in u_t is at $c = A(\xi)$ per unit of time, where $A(x)$ is a differentiable function with $A'(x) > 0$ and $A''(x) > 0$.

We assume that when $\xi_t = 0$, i.e., there is absolutely no effort in place on system maintenance, the process u_t will have a natural downward drift. We assume this downward drift to be a constant $-c'$, $c' > 0$ until u_t hits 0. This is justified by common observations in security system management: if the system does not perform regular updates, scans, and inspections, the system becomes more and more vulnerable over time.

Let ξ' be the amount of investment that is needed to counter affect the downward drift c', and that the per unit time change in u_t caused by such investment is 0. If $\xi > \xi'$, then the per unit time change in u_t becomes c.

Mathematically, the above assumption can be summarized as the following conditions that need to be satisfied by function $A(x)$: $A(0) = -c'$, $A(x) = 0$ for $x = \xi'$, and $A(x) = c > 0$ for $x > \xi'$. The increase in the security level is justified by continuous effort on fixing known vulnerabilities, strengthening authentication and encryption, etc. References on over hundreds of defense methods can be found in Cohen [2].

The counting process $\{N_t\}_{t\geq 0}$ represents the number of attempted attacks during time $(0, t]$. When an attempted

attack arrives at time t, we assume that the probability of that attack being successful is equal to $\nu_t = e^{-\alpha u_t}$. However, whether the i^{th} attempted attack is successful or not, we assume that the strength level of the system after the attempted attack will be damaged by a random variable X_i. During an attack event, the hacker may gain some information about the system mechanism and authentication methods and that a certain level of security strength is lost. This is modeled by losses $\{X_i\}_{i=1}^{\infty}$ in security level when attack arrives.

So far our security level process follows the fundamental works of a classical insurance surplus process. To further accommodate the modeling of cyber risks, we make two modifications on the process. First modification is that once ruin occurs, the surplus level returns to 0 immediately and the process continues. This implies that the security level does not remain at ruin state but restarts from 0 whenever a failure occurred. A realization of such process is shown in Figure 1. The reason for this is that it seems unrealistic to assume that the security level can remain negative. Even when a breach event occurs, the system engineers will continue to strengthen the system security over time by fixing exploited vulnerabilities and bugs.

Another modification is a loosening on the assumption for c such that the probability of ruin/breach event is not strictly less than 1 under our framework. More discussion on this modification can be found in Appendix A.

Table 1 provides a comparison between surplus process definitions under traditional ruin theory versus our cyber security framework. In reality, the cyber environment is characterized as an arms race between attackers and defenders. Perpetrators are actively searching for weak points and new methods and tools (e.g., malware) for attacking. The results of attackers are quantified by $\{X_i\}_{i=1}^{\infty}$ which emerges over time. Defenders must vigilantly monitor and constantly invest in cyber security in terms of time, knowledge, and measures. The defense spending of amount $\$\xi$ gives c as the continuous security development rate. Our focus is on the time dimension of the arms race between attackers and defenders. In this paper, we investigate how company spending in beefing up cyber security level can help maintain/achieve a desirable security level.

Let the counting process of the number of ruin events between time $(0,t]$ be $\{\mathrm{NR}_u(t)\}_{t\geq 0}$, with initial surplus u, under the modified surplus process. Let $T_{u,n}$ to be the time of n^{th} ruin event and $\omega_{u,n}(t)$ to be the probability density function of $T_{u,n}$. Define $W_{u,n}(t) = \int_0^t \omega_{u,n}(\tau)\mathrm{d}\tau = \Pr(T_{u,n} \leq t)$, we can then derive the probability function for $\mathrm{NR}_u(t)$. For $n = 0$, we have that

$$\Pr[\mathrm{NR}_u(t) = 0] = \Pr(T_u > t) = 1 - W_{u,1}(t). \tag{2}$$

Note that this also includes the probability that ruin never occurs and that by definition $W_{u,1}(t) = W_u(t)$. For $n \geq 1$,

$$\begin{aligned}\Pr[\mathrm{NR}_u(t) = n] &= \Pr\left(T_{u,n} \leq t < T_{u,n+1}\right)\\ &= \Pr\left(T_{u,n} \leq t\right) - \Pr\left(T_{u,n+1} \leq t\right)\\ &= W_{u,n}(t) - W_{u,n+1}(t).\end{aligned} \tag{3}$$

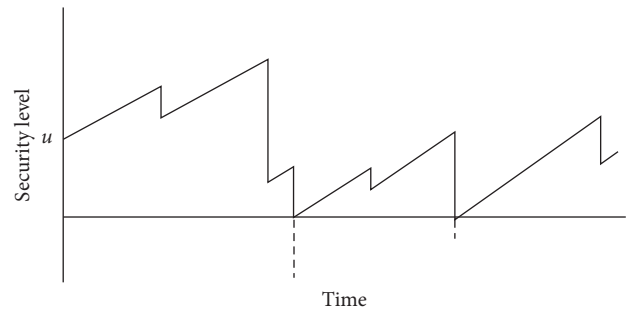

Figure 1: Security process.

Table 1: Traditional ruin theory and the proposed application on cyber security level modeling.

Notation	Traditional ruin theory	Apply to cyber security changes
U_t	Insurer's surplus level	Company's cyber security level
u	Initial surplus level	Initial level of cyber security
c	Continuous premium income	Continuous cyber security development derived from cyber security investment
N_t	Counting process of the number of claims	Counting process of the number of cyber attacks
X_i	Insurance claims	Damage to security level caused by the attacks
Ruin event	Insolvency	Cyber breach

Under our cyber risk model, we use $\mathrm{NR}_u(t)$ as the counting process for breach events. Furthermore, let $\{Y_i\}_{i=1}^{\infty}$ be independent and identically distributed random variables representing the severity of financial loss due to a security breach. We assume that $\{Y_i\}_{i=1}^{\infty}$ depends on the nature of data breached and is independent of U_t and $\mathrm{NR}_u(t)$. The total financial loss due to defense failure between time $(0,t]$ is then $\sum_{i=0}^{\mathrm{NR}_u(t)} Y_i$.

Since ξ is the amount of investment in cyber security per unit time, we denote $L(u,\xi,t)$ to be the total cyber cost between $(0,t]$ and we have

$$L(u,\xi,t) = \xi t + \sum_{i=1}^{\mathrm{NR}_u(t)} Y_i. \tag{4}$$

The expected total cyber costs between $(0,t]$ are then

$$E[L(u,\xi,t)] = \xi t + E[\mathrm{NR}_u(t)]E[Y_i], \tag{5}$$

where the expected number of breaches before t can be found as follows:

$$E[\mathrm{NR}_u(t)] = \sum_{n=1}^{\infty} n\left[W_{u,n}(t) - W_{u,n+1}(t)\right] = \sum_{n=1}^{\infty} W_{u,n}(t). \tag{6}$$

Taking the partial differentiation of $E[L(u,\xi,t)]$ with respect to ξ, we have

$$\frac{\partial E[L(u,\xi,t)]}{\partial \xi} = t + E(Y_i)A'(\xi)\sum_{n=0}^{\infty}\frac{\partial W_{u,n}(t)}{\partial c}. \quad (7)$$

Since $\partial W_0(t)/\partial c < 0$ and hence $\partial W_{u,n}(t)/\partial c < 0$, and that $A'(\xi) > 0$, we see that there exists an ξ^* such that $\partial E[L(u,\xi,t)]/\partial \xi = 0$.

Note that the expected loss $E[\mathrm{NR}_u(t)]E[Y_i]$ represents the net premium for cyber insurance cover for losses from cyber breach. The higher the IT security spending, the lower the resulting net premium of cyber insurance. There is an optimal amount of spending that minimizes the total cost to the firm. Using equation (5), firms can decide an optimal allocation of total cyber security budget to (1) IT security maintenance/upkeep spending versus (2) external cyber risk transfer. The total cyber cost function can be generalized to allow for expense loading of insurance covers. If the insurance premium is the expected financial loss $E[\mathrm{NR}_u(t)]E[Y_i]$ plus a loading θ under the expected value principle, the total cyber cost function then becomes

$$L(u,\xi,t) = \xi t + (1+\theta)E[\mathrm{NR}_u(t)]E[Y_i]. \quad (8)$$

3. Insights from the Framework

In this section, we assume a baseline scenario that $\{N_t\}_{t\geq 0}$ follows a Poisson process with parameter $\lambda = 1$, and $\{X_i\}_{i=1}^{\infty}$ follows an exponential distribution with parameter $\alpha = 1$. The initial security level is $u = U_0 = 3$. We also assume that the construction rate $c = A(\xi) = \ln(\xi + 1)$, where ξ is the amount of investment on security development. Note that under this assumption $A(0) = 0$, $A'(\xi) > 0$ and $A''(\xi) > 0$ for $\xi > 0$. The expected loss when breach occurs is assumed to be $E(Y_i) = \$20$ and the time horizon is $t = 2$. Some analytical results are given in Appendix B under these assumptions.

To further clarify the notation used, u, λ, α, and c are numerical metrics corresponding to the security level process, whereas ξ, $E(Y_i)$, and $E[L(u,\xi,t)]$ represent the monetary amounts associated with security investments and costs of cyber breaches.

In the following examples, we change various assumptions and study the impact on the expected total cyber cost $E[L(u,\xi,t)]$. Under each scenario, we find the optimal investment level ξ^* such that the expected cyber cost is minimized given the specific time horizon.

3.1. Impact of Loss Severity. In this example, we assume an alternative scenario with $E(Y_i) = \$40$. Clearly in our baseline scenario where $E(Y_i) = \$20$, the average severity of loss in an event of cyber breach is relatively low compared with $E(Y_i) = \$40$. Figure 2 shows how expected cyber costs change with respect to changes in ξ given the assumed $E(Y_i)$.

Under our baseline scenario, where $E(Y_i) = \$20$, if we invest nothing in security development such that $\xi = \$0$ and hence $c = 0$, the expected number of defense failures is 0.45. As ξ increases, we see that $E[L]$ firstly decreases until it reaches the minimum at $\xi^* = \$1.02$ with the minimized expected cyber cost at $E[L(3, 1.02, 2)]^* = \$7.22$. The expected number of defense failures given $\xi^* = \$1.02$ is 0.26. Note that with $\xi^* = \$1.02$, the corresponding $c = 0.70 < \lambda/\alpha$. This indicates that under the given conditions above, it is actually less optimal to maintain $c > \lambda/\alpha$, which is a condition needed for $\psi(u) < 1$.

For $E(Y_i) = \$40$, the minimum expected cost is \$11.65 with $\xi^* = \$1.94$. The optimal security investment is higher compared with the previous case. Table 2 provides a summary of the results above.

Insights: in the case of higher average loss severity, it is better to invest more in security defense to reduce the expected number of breach events.

3.2. Impact of Different Attack Arrivals. In this example, we look at the impact of different attack arrivals on expected cyber losses and optimal investment level ξ^*. We adopt the same baseline scenario such that $u = 3$, $\lambda = 1$ and $\alpha = 1$, $c = A(\xi) = \ln(\xi + 1)$, $t = 2$, and $E(Y_i) = \$20$. We assume two alternative sets of parameters for attack arrivals: for the first alternative scenario (scenario 2), we assume $\lambda = 0.5$ and $\alpha = 0.5$, which represents the case where the attack frequency is halved, but the expected impact is doubled due to more sophisticated attacks. For the second alternative scenario (scenario 3), we assume $\lambda = 10$ and $\alpha = 10$, which represents a high-frequency but low-impact (less sophisticated) attack for the attack arrivals.

Figure 3 shows the change in the expected number of breaches $E[\mathrm{NR}_3(2)]$ given ξ assuming different attack arrivals as above. We see that for scenario 3, $E[\mathrm{NR}_3(2)]$ decreases quickly with small increase in ξ. A small amount of investment can reduce the expected number of breaches significantly. For scenario 2, the investment is less efficient because $A''(\xi) < 0$ such that each additional unit spending of ξ causes smaller additional c and that high impact of the attacks overpowers the security improvement.

We then calculate the expected total cyber costs under the assumed three scenarios, and Figure 4 shows the changes in $E[L(3,\xi,2)]$ with respect to changes in ξ. The optimal investment ξ^* is then calculated for each scenario with corresponding results shown in Table 3.

For the baseline scenario, the optimal ξ^* is \$1.02 with the minimum expected cyber costs at \$7.22. For scenario 2, the optimal $\xi^* = \$0.38$ is smaller than the baseline scenario, with the minimum expected cyber costs higher at \$7.31. Under this scenario, the system manager actually opts to invest less due to the comparatively inefficient cyber investment. For scenario 3, the optimal $\xi^* = \$0.49$ is lower than the baseline scenario but higher than scenario 2. However, we see that the optimal expected cyber costs decreased significantly from \$7.22 and \$7.31, compared with the baseline scenario and scenario 2, respectively.

Insights: for a given expected loss amount as the product of frequency and severity, if a company's computer system is facing more frequent but less severe attacks, it is optimal for the company to invest less amount in security improvement.

3.3. Impact of Time Horizon. In previous sections, we assumed $t = 2$ for numerical illustrations. We now look at the impact of time horizon on the changes in the optimal

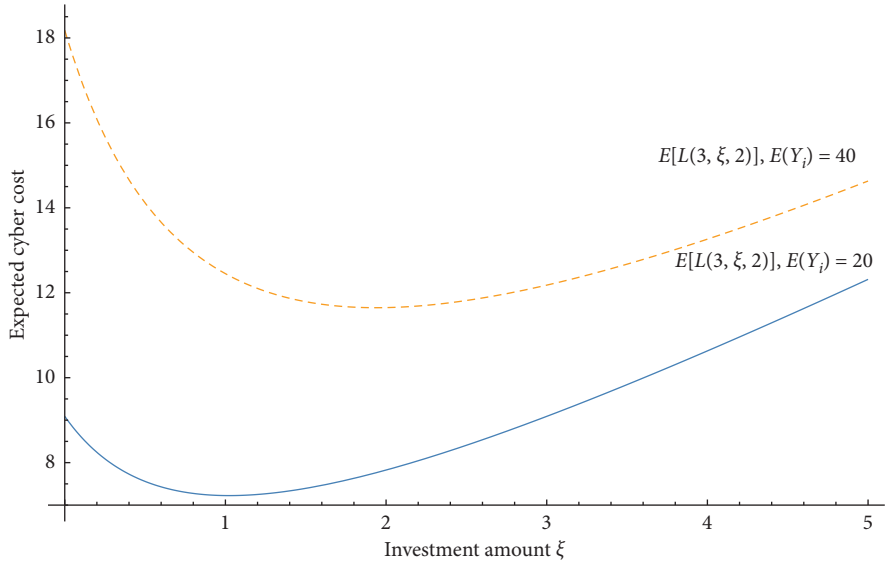

Figure 2: Total expected cyber cost with different $E(Y_i)$.

Table 2: Optimal ξ^* with different loss severity.

Expected loss per breach $E(Y_i)$	Optimal IT spending ξ^*	Insurance net premium $E[\mathrm{NR}_u(t)]E[Y_i]$	Expected cyber cost $E(L)^*$
\$20	\$1.02	\$6.20	\$7.22
\$40	\$1.94	\$9.71	\$11.65

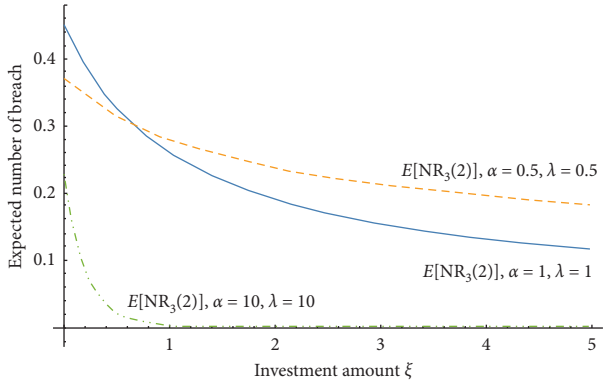

Figure 3: Expected number of breaches with different attack arrivals.

investment level ξ. We assume $u = 3$, $\lambda = 1$, $\alpha = 1$, $c = A(\xi) = \ln(\xi + 1)$, and $E(Y_i) = \$20$. Figure 5 illustrates the changes in $E[L(3, \xi, t)]$ with changes in ξ, assuming $t = 1$, $t = 2$, and $t = 5$, respectively.

Intuitively, as t increases, the expected total cyber cost shifts upward. Our interest lies in the changes in optimal investment amount when looking at different time horizons. Table 4 shows the optimal ξ^* for $t = 1$, $t = 2$, and $t = 5$, respectively. We also calculate the corresponding $E(L)^*/t$ and $E[\mathrm{NR}_3(t)]^*/t$, which represent the expected cyber cost and expected number of breaches per time unit, respectively, given ξ^*. There are a few observations from the results as follows. Firstly, as we look at longer time horizon, it is optimal to invest more in security development to reduce the total expected cyber costs. Next, the $E(L)^*$ is not linearly related to t as t changes. This is because at the end of one year, the security level may be lower or higher than the start of the year and the optimal level of investment will change accordingly for the next year. In addition, the optimal average expected number of breaches per time unit also changes when we consider different time horizons.

Insights: the choice of time horizon has important implications when deciding the optimal security spending.

3.4. Impact of Initial Security Level. In this example, we look at the impact of different initial security level u. We assume $\lambda = 1$, $\alpha = 1$, $c = A(\xi) = \ln(\xi + 1)$, $t = 2$, and $E(Y_i) = \$20$. Figure 6 illustrates the changes in $E[L(u, \xi, 2)]$ with changes in ξ, given $u = 1$, $u = 3$, and $u = 5$. We see that when ξ is small, the differences in expected cyber cost are relatively large when u changes. As ξ becomes larger, the gaps between the three lines become smaller and almost remain constant for large ξ.

In Table 5, we provide the optimal investment ξ^* and corresponding expected cyber costs. When $u = 1$, the optimal ξ^* is \$2.46 with minimum expected cyber costs at \$16.33. When $u = 5$, the optimal $\xi^* = \$0.16$ and the minimum expected cyber cost is \$2.87.

Assume we can invest ξ_a^b, $a < b$, to instantly increase U_t from a to b. We also assume that $\xi_a^b \geq A^{-1}(b - a)$. This implies that if we want to increase U_t from a to b instantly, it will cost more than develop U_t from a to b during 1 unit time. If at time $t = 0$ and $u = a$, the expected total cyber cost under previous settings will be $E[L(a, \xi, t)]$. Suppose we decide to invest ξ_a^b such that the initial u increases to b

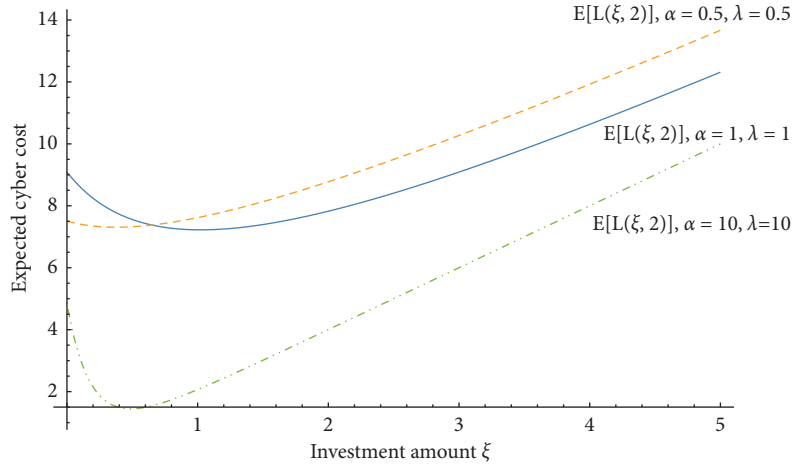

Figure 4: Total expected cyber cost with different attack arrivals.

Table 3: Optimal ξ with different attack arrivals.

Parameters	Expected cyber cost $E(L)^*$	Optimal IT spending ξ^*	Expected number of breaches $E[\mathrm{NR}_3(t)]^*$
$\lambda = 1$, $\alpha = 1$	\$7.22	\$1.02	0.26
$\lambda = 0.5$, $\alpha = 0.5$	\$7.31	\$0.38	0.33
$\lambda = 10$, $\alpha = 10$	\$1.45	\$0.49	0.02

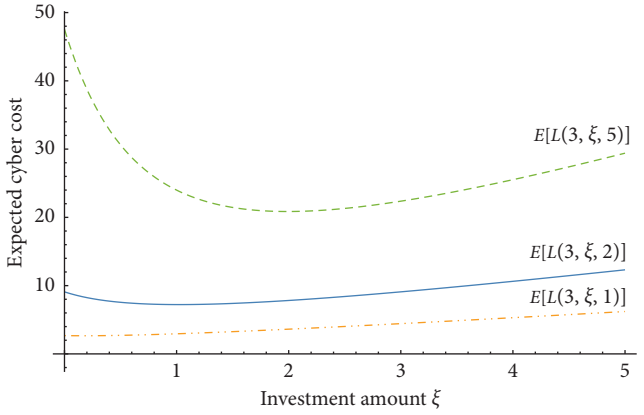

Figure 5: Total expected cyber cost with different t.

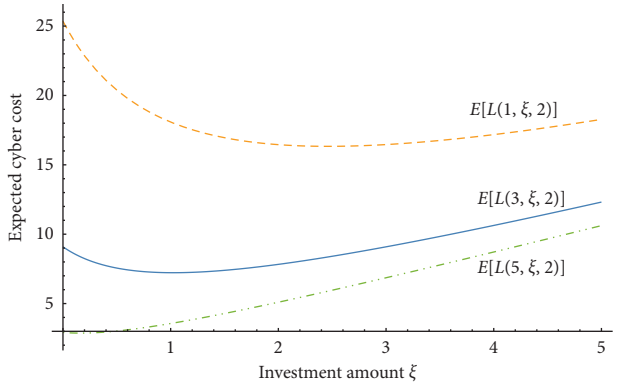

Figure 6: Total expected cyber cost with different u.

instantly and the process continues. The total cyber cost under this scenario is then $\xi_a^b + E[L(b, \xi, t)]$. From the table above, we see that $\xi_1^3 \geq \$6.39$. If $\xi_1^3 \leq \$9.11$, the firm can actually reduce the total expected cyber cost by a one-off investment to boost the initial security level from 1 to 3.

Insights: it may be worthwhile for a company to spend one-off investment from time to time to boost cyber security level to a desirable standard.

4. Literature Review on Cyber Risk Modeling

In this section, we provide a brief literature review on cyber risk modeling. The computer information system (CIS) risk had always been one of the key concerns for computer engineers. In the era of digitization, big data, and global connectivity, the requirements for cyber risks management escalate and become a key element in the risk management framework. In the computer science literature, the analysis of CIS risks has been split into development risks and security risks. Rigorous analysis methods and frameworks were designed to identify and manage critical risk factors in system development [3]. For security risks, the authors in [2, 4] provided extensive lists of potential attacks, defenses, threats, and consequences. With the effort to quantitatively analyze system security, network topology and graph are used together with epidemic models and become more popular in recent years. Li et al. [5] applied a stochastic model upon a complex network graph that includes sets of nodes and sets of edges over which direct attack can be carried out in the network. A stochastic abstraction of the interactions between the attacker and the defender in the network is considered to derive the probability that a

Table 4: Optimal ξ with different t.

Time	Expected cyber cost per time unit $E(L)^*/t$	Optimal IT spending ξ^*	Expected number of breaches per time unit $E[\mathrm{NR}_u(t)]^*/t$
$t = 1$	\$2.66	\$0.17	0.12
$t = 2$	\$3.61	\$1.02	0.13
$t = 5$	\$4.17	\$1.99	0.11

Table 5: Optimal ξ with different u.

Initial security level u	Optimal IT spending ξ^*	Insurance net premium $E[\mathrm{NR}_u(t)]E[Y_i]$	Expected cyber cost $E(L)^*$
$u = 1$	\$2.46	\$13.87	\$16.33
$u = 3$	\$1.02	\$6.20	\$7.22
$u = 5$	\$0.16	\$2.71	\$2.87

uniformly chosen node is compromised (or attacked) in the steady state. Xu and Xu [6] later extended this model by weakening some strong assumptions and provided analytical results for the desired steady-state probabilities. In 2015, Xu et al. [7] incorporated copulas in the cyber epidemic models to accommodate the dependences between the cyberattack events. Pastor-Satoras et al. [8] gave a detailed review of the vast research activity concerning cyber epidemic processes, detailing the successful theoretical approaches as well as making their limits and assumptions clear.

Another stream of research focused on economic models of security investments. For example, Gordon and Loeb [1] studied the optimal protection of information, which varies with the information set's vulnerability. Dillon and Pate-Cornell [9] developed a theoretical framework that uses a utility function to explicitly examine the tradeoffs between minimization of the probability of an IS project's failure and maximization of the expected benefits from its performance. Bohme and Moore [10] developed a dynamic model to reflect the interaction between a defender and an attacker and showed how the defender's knowledge about prospective attacks and the sunk costs incurred when upgrading defenses reactively affects the optimal security investment strategy. Many more literature studies can be found in Gordon and Loeb [11] and Wang [12]. In response to the escalating demands from companies to seek better cyber risk management, the market for insurance has emerged and evolved in recent years to provide covers on cyber-related losses. However, the industry has seen a slower pace in market expansion than anticipated due to a number of challenges. The first question is the insurability of cyber risks. Biener et al. [13] focused extensively on this matter by applying Berliner's [14] insurability framework together with empirical analysis. The first insurability criterion is the randomness of the loss occurrence and the conclusion is that it is problematic due to a number of reasons. Their paper also showed that the average loss in different industries differs due to different awareness levels and therefore different resources devoted to self-protection, and the nature of the asset being protected, for example, whether the data include sensitive personal information. The higher the expected loss, the more valuable the breached information must be and the higher the gain for the attacker. Higher frequency for attacks may be correlated to high potential loss. As a result, it may be optimal for a potential victim to spend more on security development, such that the expected total cyber cost is minimized.

Unlike traditional insured risks where the losses emerge from random events, the majority of known cyber loss events are usually consequences of failure in IS defense against intentional attacks. The losses from these attacks are quite profound, for example, the theft and leakage of SONY's internal data in 2014 caused an estimated USD 35 million loss. It is commonly believed that the company's investment on security development plays a key role in reducing the possibility of such loss [10]. Xu and Hua [15] developed a framework to model and price cyber security risk. Due to the constantly evolving technologies of both the attackers and defenders, the attempt to estimate the likelihood and severity of a cyber loss becomes even more challenging. Another obstacle for cyber insurance is the lack of historical loss data attributed to cyber losses that can be used to estimate probabilities of loss and calculate loss values [16]. The data scarcity problem has been addressed by the industry and there have been many attempts to pool relevant data for analytical purposes. Romanosky [17] used a unique dataset of over 12,000 cyber incidents recorded over the years 2004 and 2015 in the USA and examined the costs and causes of cyber incidents. It later went on to discuss the amount of capital a firm should spend on IT security.

Alternatively, one can possibly obtain data other than insurance losses for the purpose of studying cyber risks. Organizations usually have many sources of information about attacks that may be incident upon their networks [18]. One important source is firewall logs. Most, if not all, corporate networks will run a firewall that limits the traffic in and out of the corporate intranet according to some set of rules. Firewalls also log the network activity that they see, particularly the network traffic that is being dropped. Security teams examine firewall logs to get an indication of what attacks are occurring. The log files may show particular IP addresses that are running scans or particular network ports that are being attacked. A network intrusion detection system may be able to monitor and record abnormalities observed for future analysis of attack rates. Alternatively, some research studies focused on analyzing the honeypot-

captured cyberattacks to better understand the attack behaviours, for example, Spitzner [19], Almotairi et al. [20], and Zhan et al. [21].

5. Conclusion and Future Research

In this paper, we assume the security level of a system is a quantifiable metric and apply the ruin theoretic framework in assessing the defense failure frequencies. We assume that the security level of a system changes over time due to attack and defense. The security level is then modeled by a modified surplus process: the current security level of an information system can be viewed as the initial surplus; defense investment resulting in an increase in the security level can be viewed as the premium income; the cyberattack arrivals are modeled as a Poisson process; and the impact of attacks is modeled as losses on the security level using an assumed loss distribution. A cyberattack succeeds (or the defense fails) when ruin occurs. In other words, we apply the risk process to model the frequency of the cyber failure. Once the defense failed, an independent financial loss amount is incurred depending on the nature of data being breached.

To our knowledge, this is the first attempt in the literature to apply the ruin theory on IT security investments and risk modeling. Instead of modeling cyber incidence directly, we assume that attacks can occur but unsuccessful if higher security level (strong defense) is in place. We also assume that the security level erodes even if unsuccessful attack happened. This is based on our assumption that the dark web (or cyber criminals) is capable of learning from their past attempts, which leads to a decrease in security level without active upgrading on the defense side. This paper is not meant to propose a new actuarial model for cyber risks, but instead using an actuarial ruin theory framework to gain insights about optimal allocation of cyber security budget.

One important insight derived from this theoretical framework is that there is an optimal allocation of total cyber security budget to (1) IT security maintenance/upkeep spending versus (2) external cyber risk transfer. This has an implication in insurance product design: insurers may consider offer a combination of IT risk management services and risk transfer. The IT risk management services can be jointly offered with or outsourced to IT security firms. The security level is modeled as a numerical level in this paper. In practice, one can develop extensive IT risk assessment framework to produce numeric ratings. However, this is beyond the scope of this paper. When modeling the security level, we used simple models for attack frequencies (Poisson arrivals) and severity (exponentially distributed), as well as the security construction rate (constant) which may be over simplifications of what the reality represents. However, our aim for this paper is to use a theoretical framework to derive insights on cyber security budgeting. A few possibilities to alter these assumptions for future research are listed as follows:

(1) The attacks may be modeled as nonhomogeneous Poisson process. IT security level could potentially also influence the attack behaviour. The attack frequencies might be high for a period of time and low if several attempts were unsuccessful. Alternatively, one can consider using a dependent risk process model to reflect some actual dependencies between attack frequencies and severity, and such model has been studied in the studies of Peng and Wang [22] and Hu and Zhang [23]. On the other hand, some more complicated risk models can be used to model the cyber risk, such as Markov-modulated risk model, Levy risk model, and MAP risk model. Many references can be found in the studies of Asmussen and Albrecher [24], Li et al. [25], Li et al. [26], Zhang et al. [27], Cheung and Feng [28], Yu et al. [29], etc.

(2) Instead of continuous observation of the process, the security officer may wish to adopt a periodic check-up strategy and place occasional boost-ups for the security level. This strategy can then be seen as a risk process that is periodically observed with some occasional capital injections (see Yu et al. [30] and Zhang et al. [31]).

(3) We assumed that the surplus level returns to 0 immediately after breach. Further research may alter this assumption since it may require some time to clear the virus or repair the equipment.

(4) Empirical calibration of model parameters using actual data.

Appendix

A. The Security Development Rate c

For the purpose of applying the surplus process to model the cyber security level, we made a loosening on the assumption for c. Under classical risk theory, it is typical to assume $ct > E(\sum_{i=1}^{N_t} X_i)$ to ensure that ultimate ruin probability is not 1. Under our cyber risk model, it may be unrealistic to assume the same for the security construction rate. Unlike the premium rates that are mainly determined by insurers, the system engineers are usually restrained by available resources and technology and may not have as much control over c. Also, it may be more appropriate to assume that given the same amount of investment, c should be lower when U_t is large and higher when U_t is low. This is due to the constraints on existing technologies and the higher the U_t is, the more difficult it is to strengthen it using existing methods. This will then correspond to a level-dependent risk process. Without newly developed technologies, ultimately $c \to 0$ as $U_t \to \infty$. Under this argument, the ruin probability will be 1 [24]. Some ruin theory discussions on surplus-dependent premiums can be found in Albrecher et al. [32]. Other relevant papers involving discussions on varying premiums may be found in Jasiulewicz [33], Li et al. [34], and Rong and Li [35]. However, most of these papers discussed ruin-related problem assuming $ct > E(\sum_{i=1}^{N_t} X_i)$. In this paper, we assume $c = A(\xi)$ to be a function of the security investment ξ but does not depend on the surplus level. As a result, the ultimate ruin probability $\psi(u)$ is 1 for some values of ξ.

B. Some Analytical Results

In this section, we derive some analytical results assuming that $\{N_t\}_{t\geq 0}$ follows a Poisson process with parameter λ, and $f(x) = \alpha e^{-\alpha x}$. It is a well-known result [36] that the Laplace transform of T_u is found as follows:

$$\widetilde{\omega}_u(s) = \left(1 - \frac{R_s}{\alpha}\right)e^{-R_s u}, \tag{B.1}$$

where $-R_s < 0$ is a root of the characteristic equation:

$$x^2 + \left(\alpha - \frac{\lambda + s}{c}\right)x - \frac{\alpha s}{c} = 0. \tag{B.2}$$

Note that the derivation was done under the assumption that $c > \lambda E(X)$, but equation (B.1) is not affected if we relax this assumption. This is because $E[e^{-sT_u} I(T_u < \infty)] = E[e^{-sT_u}] = \widetilde{\omega}_u(s)$, and that the derivation of $\widetilde{\omega}_u(s)$ and $\omega_u(t)$ does not depend on the condition that $c > \lambda E(X)$. Dickson and Li [37] showed that the defective/proper density of T_u satisfies the following equation:

$$\omega_u(t) = \sum_{j=1}^{\infty} \omega_0^{j*}(t) \frac{(\alpha u)^{j-1} e^{-\alpha u}}{\Gamma(j)}, \tag{B.3}$$

where $\omega_0^{j*}(t)$ is the j-fold convolution of $\omega_0(t)$. From Nie et al. [38], we have

$$\omega_0^{j*}(t) = \frac{\lambda^j t^{j-1} e^{-(\lambda+\alpha c)t}}{\Gamma(j)} {}_0F_1\left(j+1; \alpha c \lambda t^2\right), \tag{B.4}$$

where

$$\begin{aligned} &{}_pF_q\left(B_1, B_2, \ldots, B_p, C_1, C_2, \ldots, C_q; Z\right) \\ &\quad = \sum_{m=0}^{\infty} \frac{(B_1)_m (B_2)_m \cdots \left(B_p\right)_m}{(C_1)_m (C_2)_m \cdots \left(C_p\right)_m} \frac{Z^m}{m!}, \end{aligned} \tag{B.5}$$

is the generalized hypergeometric function and $(a)_n = \Gamma(a+n)/\Gamma(a)$ is Pochhammer's symbol. Under the framework proposed in Section 2.2, we can derive the Laplace transform of $\omega_{u,n}(t)$ as follows:

$$\begin{aligned} \widetilde{\omega}_{u,n}(s) &= \widetilde{\omega}_u(s)\left[\widetilde{\omega}_0(s)\right]^{n-1} \\ &= \sum_{j=1}^{\infty} \frac{(\alpha u)^{j-1} e^{-\alpha u}}{\Gamma(j)} \left(1 - \frac{R_s}{\alpha}\right)^{j+n-1}. \end{aligned} \tag{B.6}$$

The defective/proper density function of $T_{u,n}(t)$ is then

$$\begin{aligned} \omega_{u,n}(t) &= \omega_u * \omega_0^{n-1*}(t) \\ &= \sum_{j=1}^{\infty} \omega_0^{j+n-1*}(t) \frac{(\alpha u)^{j-1} e^{-\alpha u}}{\Gamma(j)} \\ &= \sum_{j=1}^{\infty} \frac{\lambda^{j+n-1} t^{j+n-2} e^{-(\lambda+\alpha c)t}}{\Gamma(j+n-1)} {}_0F_1\left(j+n; \alpha c \lambda t^2\right) \\ &\quad \frac{(\alpha u)^{j-1} e^{-\alpha u}}{\Gamma(j)}. \end{aligned} \tag{B.7}$$

Note that for $c \leq \lambda E(x)$, $\Pr(T_{u,n} < \infty) = 1$ and equation (B.7) becomes a proper density function. For $c > \lambda E(X)$, we have $\Pr(T_{u,n} < \infty) = \psi(u)\psi(0)^{n-1}$ and that the conditional density function of $T_{u,n} | T_{u,n} < \infty$ becomes $\omega_{u,n}(t)/\psi(u)\psi(0)^{n-1}$.

Data Availability

No real data were used in this manuscript.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

Jingchao Li acknowledges the support from the National Natural Science Foundation of China (project no. 11601344), Shenzhen Peacock Program (project no. 000417), and Natural Science Foundation of Guangdong Province (project no. 2020A1515010372).

References

[1] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Transactions on Information and System Security*, vol. 5, no. 4, pp. 438–457, 2002.

[2] F. Cohen, "Information system attacks: a preliminary classification scheme," *Computers & Securiy*, vol. 16, pp. 29–46, 1997a.

[3] J. L. Whitten and L. D. Bentley, *Systems Analysis and Design Methods*, Irwin McGraww-Hill, New York, NY, USA, 4th edition, 1998.

[4] F. Cohen, "Information system defences: a preliminary classification scheme," *Computers & Securiy*, vol. 16, pp. 94–114, 1997b.

[5] X. Li, T. Parker, and S. Xu, "A stochastic model for quantitative security analysis of networked systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 1, pp. 28–43, 2011.

[6] M. Xu and S. Xu, "An extended stochastic model for quantitative security analysis of networked systems," *Internet Mathematics*, vol. 8, no. 3, pp. 288–320, 2012.

[7] M. Xu, G. Da, and S. Xu, "Cyber epidemic models with dependence," *Internet Mathematics*, vol. 11, pp. 69–92, 2015.

[8] R. Pastor-Satorras, C. Castellano, P. V. Mieghem, and A. Vespignani, "Epidemic processes in complex networks," *Reviews of Modern Physics*, vol. 87, no. 3, pp. 925–979, 2015.

[9] R. L. Dillon and M. E. Pate-Cornell, "Including technical and security risks in the development of information systems: a programmatic risk management model," *Systems Engineering*, vol. 8, no. 1, pp. 15–28, 2008.

[10] R. Bohme and T. Moore, "The iterated weakest link: a model of adaptive security investment," in *Proceedings of the WEIS: 8th Workshop on the Economics of Information Security*, London, UK, June 2009.

[11] L. A. Gordon and M. P. Loeb, *Managing Cybersecurity Resources: A Cost-Benefit Analysis*, McGraw-Hill, New York, NY, USA, 2006.

[12] S. S. Wang, "Integrated framework for information security investment and cyber insurance," *Pacific-Basin Finance Journal*, vol. 57, p. 101173, 2019.

[13] C. Biener, M. Eling, and J. H. Wirfs, "Insurability of cyber risk: an empirical analysis," *Geneva Papers on Risk and Insurance-Issues and Practice*, vol. 40, no. 1, pp. 131–158, 2015.
[14] B. Berliner, *Limits of Insurability of Risks*, Prentice-Hall, Englewood Cliffs, NJ, USA, 1982.
[15] M. Xu and L. Hua, "Cybersecurity insurance: modeling and pricing," *North American Actuarial Journal*, vol. 23, no. 2, pp. 220–249, 2019.
[16] PwC, *Managing Cyber Risks with Insurance*, PwC, London, UK, 2014.
[17] S. Romanosky, "Examining the costs and causes of cyber incidents," *Journal of Cybersecurity*, vol. 2, no. 2, pp. 121–135, 2016.
[18] A. Baldwin, I. Cheyas, C. Ioannidis, D. Pym, and J. Williams, "Contagion in cybersecurity attacks," in *Proceedings of the WEIS: 11th Workshop on the Economics of Information Security*, Berlin, Germany, June 2012.
[19] L. Spitzner, *Honeypots: Tracking Hackers*, Addison-Wesley, Boston, MA, USA, 2003.
[20] S. Almotairi, A. Clark, G. Mohay, and J. Zimmermann, "A technique for detecting new attacks in low-interaction honeypot traffic," in *Proceedings of the Fourth International Conference on Internet Monitoring and Protection*, pp. 7–13, Venice, Italy, May 2009.
[21] Z. Zhan, M. Xu, and S. Xu, "Predicting cyber attack rates with extreme values," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 8, pp. 1666–1677, 2015.
[22] J. Peng and D. Wang, "Uniform asymptotics for ruin probabilities in a dependent renewal risk model with stochastic return on investments," *Stochastics An International Journal of Probability and Stochastic Processes*, vol. 90, no. 3, pp. 432–471, 2018.
[23] X. Hu and L. Zhang, "Ruin probability in a correlated aggregate claims model with common Poisson shocks: application to reinsurance," *Methodology and Computing in Applied Probability*, vol. 18, no. 3, pp. 675–689, 2016.
[24] S. Asmussen and H. Albrecher, *Ruin Probabilities*, World Scientific, Singapore, 2nd edition, 2010.
[25] J. Li, D. C. M. Dickson, and S. Li, "Some ruin problems for the MAP risk mode," *Insurance: Mathematics and Economics*, vol. 65, pp. 1–8, 2015.
[26] J. Li, D. C. M. Dickson, and S. Li, "Analysis of some ruin-related quantities in a Markov-modulated risk model," *Stochastic Models*, vol. 32, no. 3, pp. 351–365, 2016.
[27] Z. Zhang, Y. Yong, and W. Yu, "Valuing equity-linked death benefits in general exponential Levy models," *Journal of Computational and Applied Mathematics*, vol. 365, p. 112377, 2020.
[28] E. C. K. Cheung and R. Feng, "A unified analysis of claim costs up to ruin in a Markovian arrival risk model," *Insurance: Mathematics and Economics*, vol. 53, no. 1, pp. 98–109, 2013.
[29] W. Yu, Y. Yong, G. Guang, Y. Huang, W. Su, and C. Cui, "Valuing guaranteed minimum death benefits by cosine series expansion," *Mathematics*, vol. 7, no. 9, p. 835, 2019.
[30] W. Yu, P. Guo, Q. Wang et al., "On a periodic capital injection and barrier dividend strategy in the compound Poisson risk model," *Mathematics*, vol. 8, no. 4, p. 511, 2020.
[31] Z. Zhang, E. C. K. Cheung, and H. Yang, "On the compound Poisson risk model with periodic capital injections," *ASTIN Bulletin*, vol. 48, no. 1, pp. 435–477, 2017.
[32] H. Albrecher, C. Constantinescu, Z. Palmowski, G. Regensburger, and M. Rosenkranz, "Exact and asymptotic results for insurance risk models with surplus-dependent premiums," *SIAM Journal on Applied Mathematics*, vol. 73, no. 1, pp. p47–66, 2013.
[33] H. Jasiulewicz, "Probability of ruin with variable premium rate in a Markovian environment," *Insurance: Mathematics and Economics*, vol. 29, pp. 291–296, 2001.
[34] S. Li, D. Landriault, and C. Lemieux, "A risk model with varying premiums: its risk management implications," *Insurance: Mathematics and Economics*, vol. 60, pp. 38–46, 2014.
[35] W. Rong and W. Li, "The probability of ruin in a kind of cox risk model with variable premium rate," *Scandinavian Actuarial Journal*, vol. 2, pp. 121–132, 2004.
[36] D. C. M. Dickson, *Insurance Risk and Ruin*, Cambridge University Press, Cambridge, UK, 2005.
[37] D. C. M. Dickson and S. Li, "Finite time ruin problems for the Erlang(2) risk model," *Insurance: Mathematics and Economics*, vol. 46, pp. 12–18, 2010.
[38] C. Nie, D. C. M. Dickson, and S. Li, "The finite time ruin probability in a risk model with capital injections," *Scandinavian Actuarial Journal*, vol. 4, pp. 301–318, 2015.