INSURANCE VERSUS INVESTIGATION DRIVEN APPROACH FOR THE COMPUTATION OF OPTIMAL SECURITY INVESTMENT

Yosra Miaoui, Communication Networks and Security Research Lab, University of Carthage, Tunisia, yosra.miaoui@gmail.com

Noureddine Boudriga, Communication Networks and Security Research Lab, University of Carthage, Tunisia, noure.boudriga2@gmail.com

Ezzeddine Abaoub, College of Adminstrative and Financial Sciences, Taif University, Kingdom of Saudi Arabia, abaoub.ezzeddine@planet.tn

Abstract

Several research works have proposed economic and financial models to determine the optimal amount of investment in the security of information systems, showing the use of diverse techniques such as Game Theory (Grossklags et al. 2008), Utility Mdodels (Huang and Behara 2013; Miaoui et al. 2014), Return on Information Security Investment (Sonnenreich 2006), and Value at Risk (J. Wang et al. 2008). While many of these works showed the importance of investing in both self-protection and Cyber insurance (to reduce and transfer the residual risk of loss to insurance companies), none of them has considered the importance of security investment in forensic investigation to support insurance claims, ensure a better reimbursement of loss in case of security breach, and increase the return of investment in security.

We propose in this paper to distribute the investment in information security into investment in Self-Defense to protect against security attacks, investment in Insurance to transfer the residual risk of loss to insurance companies, and investment in Forensic Readiness to maximize the firm's potential to collect appropriate digital evidence, and generate provable insurance claims about occurred security breaches. An economic model based on the theory of utility is designed to compute the optimal total investment, taking into consideration the interdependence between the aforementioned three investments. An analysis is conducted to assess the variation of the optimal investments in self-defense and forensic readiness, and the cost of residual risk, with respect to the rate of insurance reimbursement, security vulnerabilities, and potential financial loss.

Keywords: Financial Security, Optimal Investment, Information Security, Forensics readiness, Risk Minimization, Cyber Security Insurance.

1 Introduction

Decision makers are compelled to invest in information security to reduce the likelihood of security breaches on business and IT operations. Focusing only on implementing well-known techniques and good practices of security (e.g., maintaining security patches up to date) will certainly reduce the risk of potential losses, but will neither help enterprises determining and mitigating the root causes of attacks, nor identifying their origins and generating the evidentiary data to prosecute attackers. Therefore, investing in the design of a suitable digital forensic investigation strategy is a key element in increasing the return of a security investment.

A security investment includes the security measures that mitigate the risk of attacks and potential loss, including security policy development, architectures design, and security solutions deployment. Making a decision to determine the optimal amount of security investment (i.e., the amount which maximizes the Esperance of the gained loss, and minimizes the risk of attack) is a complex task, as it requires: a) looking for a compromise between the residual risk of loss, and the amount of investment, knowing that it is almost impossible to make a system perfectly secure using a finite amount of investment; b) shifting expenditures in self-protection to mitigate the security risk, and expenditures in insurance to transfer the risk to insurance companies and to reduce the potential financial loss; and c) coming to a compromise between investments in enterprise protection, investigation measures, and insurance contracts to increase the overall protection level and the investigation capabilities of the enterprise, while reducing the residual risk of loss.

Several research works on security investments were proposed in the literature. In (Gordon and Loeb 2002) and (Huang and Behara 2013) a model that maximizes the difference between the expected amount of reduced loss and the cost of investment was proposed, taking into consideration different forms of functions to model breach probability with respect to security investment (Hausken 2006; S. L. Wang et al. 2011; Willemson 2010). These works did not consider the economic benefits for investing in cyber insurance to reduce the residual risk of loss and transfer it to insurance companies. In (Sonnenreich 2006), new techniques to compute the Return on Information Security Investment (ROSI) were proposed. All of the aforementioned works did not consider the dynamic aspects of threats and vulnerabilities over time, as their variation may affect the efficiency of the invested security solution during the investment horizon. In (J. Wang et al. 2008), the use of value-at-risk (VaR) concept was introduced, helping managers to make investment decision while considering their risk preference, instead of only focusing on the minimization of the expected loss. In (Hausken 2014) a model, which endogenizes the value of information sets, was proposed to help firms deciding how to balance resources between production versus security, considering a limitation of the budget. Aware of the dynamic aspect and variation of the threats and vulnerabilities over time, recent models were proposed to determine the optimal amount of security expenditure to keep the system secure over the whole investment horizon (Miaoui et al. 2014), and to determine the optimal timing of security investments (Ioannidis et al. 2013). The latter works did not devote importance to the minimization of the residual risk from an optimal security investment . The research works (Ogut et al. 2005) and (Bolot and Lelarge 2008) studied the impact of investment in cyber insurance on the cost and efficiency of security investments, and also on the increase of incentives to invest in self-protection. In (Grossklags et al. 2008) a game theory model was proposed to shift between expenditures in

self-protection and in cyber insurance. The last cited works did not consider the importance of the simultaneous investment in both cyber insurance and forensic digital investigation. In fact, by using forensic investigation mechanisms, enterprises become able to collect the required evidence, analyze an incident, repair it, and prove the source and steps of the executed attack. They could obtain advantageous insurance premiums, and high reimbursement rates.
We propose in this work to develop a financial model for the computation of the optimal amount of investment in information security, considering three types of interdependent investments; namely self-defense security, forensic investigation readiness, and cyber insurance. A two-step based approach for computing the optimal amount of investment, using the utility theory, is proposed. In the first step, we determine the optimal investment in self-defense security capable of reducing the risk of security breaches given the monetary value of loss and the rate of security vulnerabilities and threats. In the second step, our proposed model aims to reduce the probability of non-investigable security breaches, and to optimize the cost of investment in forensic investigation readiness, assuming that an optimal self-defense investment is done, and that a cyber-insurance contract is proposed to the firm. An analysis is conducted to assess the variation of the optimal investments in self-defense and forensic readiness, and the cost of residual risk, with respect to the rate of insurance reimbursement, security vulnerabilities, and potential financial loss.
Our contributions is four-fold. First, to the best of our knowledge, this paper is the first attempt to address the optimal security investment problem, while taking into consideration the forensic investigation needs. Second, our approach estimates the optimal investment for an investigation system, considering the insurance cost, the level of reimbursement, and the investment in the enterprise protection. Third, we propose a new Cyber insurance policy, which considers the evidentiary aspect of the provided traces when reimbursing a loss occurred due to a Cyber attack. Fourth, we propose a new concept called the non-investigability breach, which measures the capacity of the firm to investigate security attacks related to a given vulnerability, and to increase the evidentiary aspect of the claims presented to the insurers (to get a high reimbursement rate).
This paper is organized as follows. Section 2 describes the models related to insurance reimbursement, security investment, and breach investigability. In Section 3 we use the utility theory to model the optimal security investment problem with cyber insurance and forensic capability. In Section 4 we solve optimal security investment problem, and deduce the residual risk of loss. Section 5 focuses on the analysis of the obtained results. The last section concludes the work.

2 Cyber insurance, security investment, and non-investigable breach probability

In this section we focus on the design of a cyber insurance policy, and the modeling of security investments and a non-investigable security breaches.

2.1 A new cyber insurance policy aware of the evidentiary aspect of traces

The recent works on optimal security investment in insurance did not consider the impact of investment in forensic investigation readiness (to maximize the firm's potential to collect and use appropriate digital evidence, and to minimize the cost of investigation), on the cost and

Return on Investment (RoI) of a security project. In fact, by motivating applicants to invest in forensic readiness procedures and tasks, insurance companies could better protect themselves from moral hazard and adverse selection, and increase the likelihood of catching attackers in the network, which in turn reduces the residual security risk incurred by companies interconnected over insecure networks. Moreover, by investing in digital forensic investigation, enterprises could provide insurance claims with credible and reliable proofs, benefit from a high rate of loss reimbursement or receive insurance premium discount.. Insurers should discourage a firm, which paid an insurance premium, from lack of incentives to take the suitable measures to protect its information system from attacks. Therefore, a high premium or a low coverage (e.g., use of deductibles) should be applied to firms that do not take the appropriate measures to reduce the probability of loss, or that are unable to prove that the incident is not self-generated.

We define in this work a model of insurance, from the insurer's perspective, which promotes the investment in digital forensic readiness. Let L be a potential fixed loss faced by the firm, and P be the insurance premium that should be paid to cover the risk of that loss. The latter (P) is set by the insurer after assessing the security risk facing the information and communication system (i.e., a security audit to assess security threats and vulnerabilities is required). We set $P = (1+\beta)\,\phi\,L$, where ϕ is the probability of a security breach; and $\beta > 0$ is the loading factor allowing the insurer to make a positive profit. The value of β depends on the competitiveness of the insurer in the market and on the degree of attractiveness of the enterprise's resources to attackers. For example, attackers could be motivated to attack firms which are either leaders on the market, or offer sensitive services. Once a security loss L is faced by the enterprise and an insurance claim is presented, the insurance reimburses: a) L if the security breach is investigable; or b) λL if the security breach in non-investigable, where λ is the reimbursement rate $0 \leq \lambda \leq 1$.

A security breach is investigable if a forensic sound collection and analysis of evidence can be conducted by the firm, allowing to prove the root cause of the incident, the main executed actions, and the sources and identities of the attackers. Based on the results of the investigation, the insured firm can provide the evidence allowing to prosecute the identified attackers. In such a case, the insurance company reimburses the whole loss L to the firm. Then, it takes the necessary measures to prosecute attackers on behalf of the insured firm.

A security breach in non-investigable if a digital investigation cannot be conducted by the firm, or it is inconclusive. Such a result can be obtained due to several reasons,. For example: i) the attacker made his/her identity undetectable (e.g., connection establishment using anonymisation proxies); ii) the attacker executed anti-forensic actions to alter/delete/hide the evidence generated on the compromised system; iii) no suitable measures were undertaken to secure traces to evidential standard of admissibility; or iv) investigators made mistakes in collecting evidence from the compromised system. The insurance company reimburses the compromised company an amount of money proportional to the occurred damages further to the execution of malicious actions.

2.2 A model for investment in information and communication security

Investing into security to protect firms' information systems from cyber threats aims to both reduce the risk of breach occurrence, and also to minimize the potential risk of monetary loss once a security attack succeeds to happen. We model the total security investment I as a sum of

three terms: $I = S + F + P$. These terms are explained below.

a) Investment in Self Defense (S): Consists in designing and deploying the security mechanisms, techniques, and solutions, necessary to protect against, detect, and respond to security attacks. Examples of such mechanisms include, but are not limited to, the design of a security policy, the use of encryption, and the access control to networks and systems.

b) Investment in Forensic Readiness (F): Consists in taking the technical and non-technical measures to make the enterprise capable of conducting a conclusive digital forensic analysis, which is compliant with the available regulatory and legal frameworks, once an incident occurs. Such an investment will increase the likelihood of generation of insurance claims that have a high evidentiary value, allowing to prove with a high confidence that the attack is not self generated, identify the source of the attack, and determine the steps of the attacks and the root cause vulnerabilities. Forensic readiness measures include, but are not limited to, a) the deployment of monitoring tools to securely collect the useful evidences and protect them against unauthorized access; b) the acquisition of evidence analysis tools; and c) the training of security personnel to conduct a digital forensic investigation and establish an interface with law enforcement.

c) Investment in insurance (P): Consists in paying an Insurance Premium to hedge the enterprise against the risk of potential loss, while transferring that risk to an insurance company.

While investment in Self defense reduces the likelihood of breach occurrence, it does not prevent potential security loss once a breach occurs. Therefore, the investment in insurance will minimize the financial loss induced by these breaches. The investment in Forensic Readiness increases the likelihood of reimbursing the whole amount of the occurred damage, by the insurance company. The model considers that the decision-maker's objective is to find the optimal total amount of security investment to reduce the potential loss due to security attacks, and find the appropriate balance between investment in Self Defense and investment in Forensic Readiness.

Even if most of security solutions are able to collect log and audit files, which provide enough details on the source of detected events, they cannot substitute an investment in forensic readiness. In fact, an additional investment is usually required to prepare the staff to protect and efficiently use the collected evidence, and design the technical and physical procedures to make evidence collection and protection compatible with the standards, and admissible in a court of law. Collecting IP addresses by a self-defense solution, for example, is insufficient to prepare for an investigation, as such an information could be forged. An investment in appropriate tools for collecting marks at different locations in the infrastructure and tracing back connections, is required.

2.3 Modeling security breach and non-investigable breach probabilities

We introduce $m \in [0,1]$ as the probability that identified security threats exploit vulnerabilities on the firm's assets (e.g., data, services, communication facilities). A security threat represents a danger (e.g., virus, natural disaster) or a trouble that causes damages. We denote by $v \in [0..1]$ the rate of vulnerability of the firm's assets against the identified threats. A vulnerability is a security weakness (e.g., weak password) in design, implementation, security policy, or internal controls. The aim of a security investment in Self Defense S is to reduce the probability (described by function $\phi(v,m,S)$) of attack. Such a function should be continuously twice differentiable for $0 \leq v \leq 1$ and $0 \leq m \leq 1$, and should also satisfy these properties:

- $\phi(v,m,0) = v \times m, \forall v, m$: As v is independent from m, the probability of security breach, in the absence of self-defense security investment, is equal to the product of v and m. In fact, a security attack, requires that a threat exploits a security vulnerability.

- $\phi(v,m,S) = 0 \Leftrightarrow S = \infty, \forall v > 0, m > 0$: The risk related to a security breach cannot be reduced to zero, unless an infinite monetary value is invested.

- $\frac{\delta\phi(v,m,S)}{\delta S} \leq 0$ and $\frac{\delta^2\phi(v,m,S)}{\delta S^2} \geq 0, \forall S$: The increase of S leads to the decrease of breach probability, and the reduction of the marginal improvement in security.

Several functions modeling the breach probability in terms of investment were investigated in the literature. In this work we consider a form which is widely used to model targeted attacks (Gordon and Loeb 2002; Huang, Hu, et al. 2008). We obtain:$\phi(v,m,S) = \frac{vm}{(1+k_1 S)}$, where $k_1 \in [0,1]$ denotes the effectiveness of the used self-defense security solution. To distinguish between investigable and non-investigable security breaches, we define the non-investigability probability function: $\rho(u,r,S,F) = \frac{u \times r}{1+k_1 S k_2 F}$, where F describes Investment in Forensic Readiness, and k_2 is the effectiveness of the forensic readiness solution. u and r are defined as follows.

a) Evidentiary rate of the attack ($u \in [0,1]$): The rate at which the conducted attack can be accurately investigated. As attacks use different techniques and tools, they are not all investigable using the same convenience. A Traffic flooding Denial of Service (DoS) attack, which consists in generating an intensive rate of incomplete service requests (allowing to identify the attacker's source) to disrupt the victim resources, shows a higher evidentiary rate than a passive traffic listening attack, which passively capture the exchanged traffic to extract sensitive information.

b) Subversion Rate ($r \in [0,1]$): The rate at which the attacker tried to divert the digital forensic process, to avoid being detected, identified, and traced. Different anti-forensic techniques (Chandran and Yan 2014) can be used, including, but are not limited to: a) logs wiping; b) use of anonymization and spoofing techniques to hide the source identity of the malicious entity; and c) hiding data in invisible slack space.

The more the value of $\rho(u,r,S)$ is close to 1, the less investigable will be the attack. The function ρ is decreasing in both S and F, and is linear in both u and r. When $S = 0$, investment in F has no effect on the non-investigability probability. In fact, we cannot imagine an investment in forensic readiness without a prior investment in self defense. Moreover, we assume that an investment in S would also reduce ρ as several self defense security solutions promotes evidence collection.

3 Modeling the optimal security investment problem

We consider that determining the optimal security investment with investigation capability should be addressed through a two-model problem. In the first model, the optimal investment problem is stated for the computation of optimal security investment in self defense capable of reducing the risk of attack occurrences. In the second model, the optimal cost of investment in forensic readiness is computed assuming that a security solution is already designed (whose cost is solved by the first problem) and that a cyber insurance is proposed.

3.1 Modeling optimal investment in self defense

The first problem consists in determining the optimal investment in self defense S. For this purpose, we propose to use the expected utility theory, which is based on the maximization of a decision-maker's wealth considering his attitude toward risk. In this work, we assume that the decision maker is risk averse (Huang, Hu, et al. 2008; Miaoui et al. 2014), as such a type of investors are the most likely to invest in information and communication security. We defined by $U(w)$ the utility function which describes for a given decision maker, its wealth preference and attitude towards risk. We assume that $U(\,)$ is continuous and twice-differentiable to wealth, and that $U'(w)$ is positive as the utility is expected to increase with wealth, and the investor is never satiated Pratt 1964. As in this work, we consider the case of Constant Absolute Risk Aversion (CARA), we have: $U(w) = \gamma - \alpha e^{-\alpha w}$ where γ is a constant, and α is a positive coefficient of absolute risk aversion, which is defined as $\alpha = -U''(w)/U'(w)$. Let L be a fixed loss incurred by the firm, whose information and communication system is attacked. We define the random variable X modeling the potential loss to be equal to L with probability ϕ (i.e., security breach has occurred), or 0 with a probability $1-\phi$ (i.e., no security breach has occurred). The expected utility related to the decision of investment in self defense solution , which is taken by a risk-averse decision maker can be expressed as: $E\left[U(w-S-X)\right] = \phi U(w-S-L) + (1-\phi)U(w-S)$. Since a decision maker wants to maximize the expected utility, the optimal security investment in self defense which we denote by $\bar{S}$, will be a solution to the following equation: $\frac{\delta}{\delta S}\left(E\left[U(w-S-X)\right]\right) = 0$.
In this work, the use of the utility theory is prompted by the findings we obtained in Miaoui et al. 2014, where the behavior of attackers is captured by the evolution of vulnerabilities over the investment horizon (which we estimated based on a regression conducted over a 14-year data history). We choose to not use the game theory, as we believe that such a type of theory requires modeling a large number of attackers, which differ by their skills, ability to execute sophisticated attacks, and types of vulnerabilities they are motivated to exploit.

3.2 Modeling optimal investment in forensic readiness

In the second step, we assume that an investment $\bar{S}$ in self-defense solution is invested, and a residual risk of breach $\bar{\phi}$ (i.e., ϕ while setting $S = \bar{S}$) is obtained. We compute the optimal investment in forensic readiness, assuming that an insurance contract is proposed. The optimal insurance premium $\bar{P}$ stated by the insurance company will be equal to: $\bar{P} = (1+\beta)\bar{\phi}L$. We assume that a potential attack on the firm's information system, which incurs a loss L, will have the probability ρ to be non-investigable. We introduce the random variable Y modeling the insurance reimbursement to be equal to L with probability ρ (i.e., the attack is non investigable), and to λL with a probability $1-\rho$ (i.e., the attack is investigable). Considering the obtained $\bar{S}$ and $\bar{P}$, the expected utility related to the investment in forensic readiness F by a risk-averse decision maker, will be: $E\left[U(w-\bar{S}-F-\bar{P}+Y)\right] = \rho U\left[w-\bar{S}-F-\bar{P}+\lambda L\right] + (1-\rho)\left(U\left[w-\bar{S}-F-\bar{P}+L\right]\right)$. When replacing $U(\,)$ by its expression, we obtain:

$$E\left[U(w-\bar{S}-F-\bar{P}+Y)\right] = \rho\left[\gamma-\alpha e^{-\alpha\left(w-\bar{S}-F-\bar{P}+\lambda L\right)}\right] + (1-\rho)\left[\gamma-\alpha e^{-\alpha\left(w-\bar{S}-F-\bar{P}+L\right)}\right] \quad (1)$$

As a decision maker wants to maximize the expected utility through the total security investment, the first-order equilibrium can be obtained by $\frac{\delta}{\delta F}\left(E\left[U(w-\bar{S}-F-\bar{P}+Y)\right]\right)=0$. We obtain:

$$-\alpha e^{-\alpha w+\alpha\bar{S}+\alpha\bar{\phi}L(1+\beta)}\left[\frac{\delta\rho}{\delta F}e^{\alpha F-\alpha\lambda L}+\alpha\rho e^{\alpha F-\alpha\lambda L}+\alpha e^{\alpha F-\alpha L}-\frac{\delta\rho}{\delta F}e^{\alpha F-\alpha L}-\alpha\rho e^{\alpha F-\alpha L}\right]=0 \quad (2)$$

Since $\alpha>0$, we have: $\frac{\delta\rho}{\delta F}e^{-\alpha\lambda L}+\alpha\rho e^{-\alpha\lambda L}+\alpha e^{-\alpha L}-\frac{\delta\rho}{\delta F}e^{-\alpha L}-\alpha\rho e^{-\alpha L}=0$. The optimal Forensic readiness investment, which we denote by $\bar{F}$, will be a solution to the latter equation.

4 Solving the optimal security investment problem

In this section we derive the mathematical expressions of the optimal security investments $\bar{S}$, and $\bar{F}$, and the residual risk of loss further to investment in insurance and forensic readiness.

4.1 Solving the first optimization problem

Solving the first problem was addressed in (Huang, Hu, et al. 2008), and later in (Miaoui et al. 2014) by considering a dynamic variation of the expression of v over time. We obtain the solution $\bar{S}$ after replacing $U(\,)$ by its expression. We get: $-\alpha e^{-\alpha(w-S)}(\frac{\delta\phi}{\delta S}e^{\alpha L}+\alpha\phi e^{\alpha L}-\frac{\delta\phi}{\delta S}+\alpha(1-\phi))=0$. Since $\alpha>0$, we have: $\frac{\delta\phi}{\delta S}(e^{\alpha L}-1)+\alpha\phi(e^{\alpha L}-1)+\alpha=0$. By replacing ϕ and $\frac{\delta\phi}{\delta S}$ by their expressions, solving the obtained quadratic equation, and discarding the negative solution of $\bar{S}$ (only the solution which is always positive is retained), we obtain:

$$\bar{S}=\frac{1}{2\alpha k_1}\left(-2\alpha-\alpha vm(e^{\alpha L}-1)+\sqrt{[\alpha vm(e^{\alpha L}-1)]^2+4\alpha k_1 vm(e^{\alpha L}-1)}\right) \quad (3)$$

From the optimal security investment, we deduce the optimal risk of security breach $\bar{\phi}$:

$$\bar{\phi}=\frac{vm}{k_1\bar{S}+1}=\frac{2\alpha vm}{-\alpha vm(e^{\alpha L}-1)+\sqrt{[\alpha vm(e^{\alpha L}-1)]^2+4\alpha k_1 vm(e^{\alpha L}-1)}} \quad (4)$$

4.2 Solving the second optimization problem

To solve the second problem taking into consideration the optimal investment in self defense $\bar{S}$, we replace ρ and $\frac{\delta\rho}{\delta F}$ by their expressions to obtain:

$$\alpha e^{-\alpha L}\left(k_1k_2\bar{S}F+1\right)^2+\left(\alpha ure^{-\alpha\lambda L}-\alpha ure^{-\alpha L}\right)\left(k_1k_2\bar{S}F+1\right)-k_1k_2\bar{S}ure^{-\alpha\lambda L}+k_1k_2\bar{S}ure^{-\alpha L}=0 \quad (5)$$

By solving the quadratic equation, we obtain:

$$k_1k_2\bar{S}F+1=\left(-\alpha ure^{-\alpha\lambda L}+\alpha ure^{-\alpha L}\pm\sqrt{\left(\alpha ure^{-\alpha\lambda L}-\alpha ure^{-\alpha L}\right)^2-4\alpha e^{-\alpha L}\left(-k_1k_2\bar{S}ure^{-\alpha\lambda L}+k_1k_2\bar{S}ure^{-\alpha L}\right)}\right)/\left(2\alpha e^{-\alpha L}\right) \quad (6)$$

Since $\alpha>0$ and $k\bar{S}F+1$ should be always positive, we discard the negative term to obtain:

$$\bar{F}=\left(-\alpha ure^{-\alpha L}(e^{\alpha(1-\lambda)L}-1)+\sqrt{\left(\alpha ure^{-\alpha L}(e^{\alpha(1-\lambda)L}-1)\right)^2+4\alpha e^{-\alpha L}k_1k_2\bar{S}ure^{-\alpha L}(e^{\alpha(1-\lambda)L}-1)}-2\alpha e^{-\alpha L}\right)/\left(2k_1k_2\bar{S}\alpha e^{-\alpha L}\right) \quad (7)$$

A risk averse decision maker is not willing to invest in a forensic reediness solution if the cost of that solution exceeds the potential value of insurance reimbursement in the case of a security breach. Since $\bar{F}$ is always positive, we have:

$$-\alpha ure^{-\alpha L}(e^{\alpha(1-\lambda)L}-1)+\sqrt{\left(\alpha ure^{-\alpha L}(e^{\alpha(1-\lambda)L}-1)\right)^2+4\alpha e^{-\alpha L}k_1k_2\bar{S}ure^{-\alpha L}(e^{\alpha(1-\lambda)L}-1)}-2\alpha e^{-\alpha L}>0 \quad (8)$$

After rearranging terms, and simplifying the expression we obtain:

$$\bar{S} > \frac{1}{k_1 k_2 ur\left(e^{\alpha(1-\lambda)L}-1\right)}\left[\left(\alpha+\alpha ur(e^{\alpha(1-\lambda)L}-1)\right)\right] \tag{9}$$

We denote the right term of expression 9 by $\bar{S}_{min}$. Therefore, if the optimal investment in Self Defense does not exceed the value $\bar{S}_{min}$, decision makers find that investment in forensic readiness would not be financially cost-effective. Having computed $\bar{S}$ and $\bar{F}$, we obtain:

$$\bar{\rho} = \frac{ur}{k_1 k_2 \bar{S}\bar{F}+1} = \frac{2\alpha vm}{-\alpha vm(e^{\alpha L}-1)+\sqrt{[\alpha vm(e^{\alpha L}-1)]^2+4\alpha k_1 vm(e^{\alpha L}-1)}} \tag{10}$$

The total optimal security investment $\bar{I}$ can be written as: $\bar{I} = \bar{S}+\bar{F}+\bar{P}$. We define by $\bar{R} = \bar{\phi}\bar{\rho}L(1-\lambda)$ the optimal residual risk of loss obtained after investing $\bar{I}$. We remind that according to the insurance reimbursement policy, the two potential losses incurred by the firm due to a security breach, which occurs with probability ϕ, will be (1) *zero* (with probability $(1-\rho)$) when there is no attack or when the attack occurs and is investigable; and (2) $(1-\lambda)L$ (with probability ρ) when the attack occurs and it is not investigable (in this case the insurer reimburses a part of the potential loss λL and therefore the enterprise potential loss is $L-\lambda L$).

5 Analysis

We analyze in this section the impact of security and insurance parameters on the breach probability and the residual risk, and also on the optimal investments in Self-Defense and in Forensic Readiness. In the sequel, we set $\alpha = 0.1$, $\beta = 0.2$, $u = r = 0.2$, $k_1 = k_2 = 0.2$, and $m = 0.3$.

Analysis of the optimal investment in forensic readiness with respect to vulnerability rate: We analyze in Figure 1 the variation $\bar{F}$ with respect to v, for different value of λ. The loss L is set to 60 monetary units. We notice an increasing evolution of $\bar{F}$ with respect to v, and a convergence towards an asymptotic value. From the economic perspective, a risk averse decision maker does not find an interest to increase the investment in forensic readiness, when his/her system becomes highly vulnerable. In fact, with respect to the expression of ϕ and ρ, as the marginal improvement in security decreases when the investment increases, the cost-benefit of the investment becomes lower and lower. Moreover, the investment in forensic readiness is not recommended for very low vulnerable systems, as a decision maker does not find it appropriate to invest in forensic readiness unless the expected risk of loss due to non-investigable breaches exceeds the cost of the insurance premium and the self defense solution. Moreover, the value of $\bar{F}$ does not exceed 5% of the expected monetary loss ($L = 60$) for extremely vulnerable systems, which encourage decision makers to invest in Forensic Readiness, and benefit from a high insurance reimbursement rate.
By increasing λ, not only the value of $\bar{F}$ decreases, but also v_{min} (the minimal value of v under which $\bar{F} = 0$) becomes higher and higher. Moreover, by increasing λ, both of the marginal differences of the minimal value of v, and the obtained optimal investments in forensic readiness, are increasing. This statement is justified by the fact that decision makers found it less and less useful to invest in the forensic readiness when the insurance company is ready to reimburse a larger portion of the incurred loss. Finally, for highly vulnerable information and communication systems, and one chosen value of λ, the investment $\bar{F}$ is almost the same.

Analysis of the optimal investment over potential loss, with respect to potential loss:

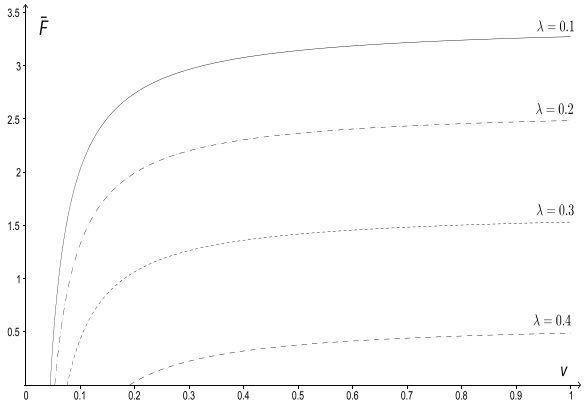
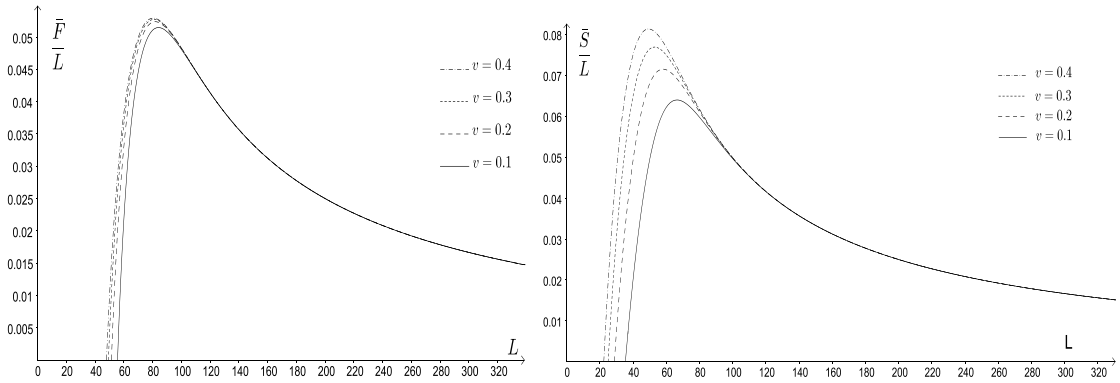


Figure 1: Optimal Investment $\bar{F}$ w.r.t. Vulnerability rate v for different reimbursement rates λ



(a) $\bar{F}/L$ w.r.t Loss L (b) $\bar{S}/L$ w.r.t Loss L

Figure 2: Optimal Investment over Loss L w.r.t Loss L

We analyze in Figure 2 the evolution of $\bar{F}/L$ and $\bar{S}/L$ with respect to L. We notice that the two ratios remain zero until the potential loss reaches a certain value. Starting from the latter value, the two ratios increase substantially with the increase of L, until a peak value is reached. After that, they start to decrease given the fact that the optimal investment in $\bar{S}$ and $\bar{F}$ do not continue to increase with the increase of loss L (as both of $\bar{S}$ and $\bar{F}$ coverage toward an asymptotic value). From the economic perspective, while the increase of L stops to affect the value of $\bar{S}$, especially for high values of L, the occurrence of a potential breach will incur a high loss. In this context, the investment in $\bar{F}$ will allow the firm to be reimbursed from insurance companies with a high rate. We notice that a firm remains protected against loss using a low ratio $\bar{F}/L$ which does not exceed 5.5%. The above conclusions are valid for different values of v. By increasing v the value of the reached peak would increase as a higher investment in self defense or forensic readiness is required, but for a larger value of L the rate is almost the same, meaning that the same value of $\bar{S}$ or $\bar{F}$ is spent for any vulnerability rate. Finally, we notice that even if the value of $\bar{F}$ will not continue to increase with the increase of loss, the insurance premium will keep increasing as it

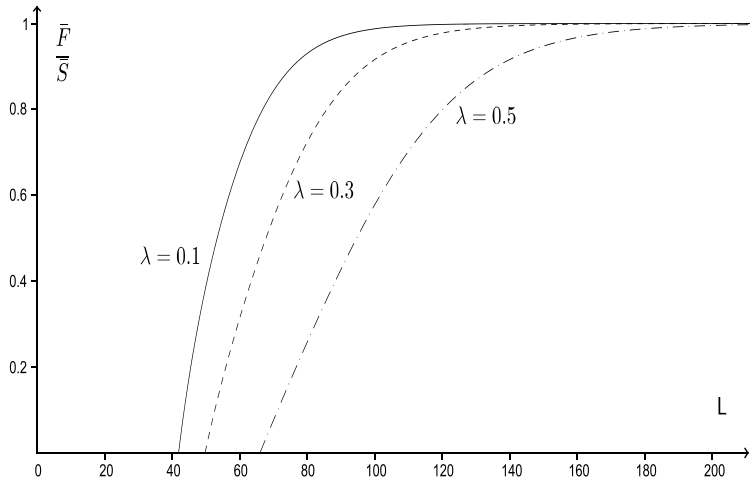


Figure 3: Evolution of the rate $\bar{F}/\bar{S}$ w.r.t. potential Loss (L)

depends on the value of L, while keeping the firm protected against very important losses.

Effect of the reimbursement rate on the evolution of the ratio $\bar{F}/\bar{S}$ with respect to L:

We propose to analyze in Figure 3 the evolution of the ratio of $\bar{F}/\bar{S}$ with respect to potential loss L, for different values of λ. We noticed that the rate $\bar{F}/\bar{S}$ increases with the increase of loss, and converges asymptotically to 1, for different values of λ. The minimal value of L (at which the investment in $\bar{F}$ starts to increase) increases with the increase of loss, and the observed marginal difference is also increasing as long as λ is increasing. We also notice that, to provide an optimal coverage against potential risk of loss, and avoid catastrophic losses (when L is very high) if a breach occurs, a firm has only to increase the amount of security investment by 100% (as the rate converges to 1). Such an increase will not affect the decision maker's wealth if we compare the amount of $\bar{F}$ with respect to loss (as seen in Figure 2a).

Analysis of the residual risk evolution with respect to vulnerability rate in the case of under-investment and over investment in self-defense:

As among the objectives of the decision makers is to reduce to the maximum possible the residual risk of loss after investing $\bar{I}$, we propose in Figure 4 to examine the evolution of the residual risk $\bar{R}$ with respect to v in the case of under-investment and over-investment in self-defense. In the following analysis, the values of L and λ are set to 50 and 0.1, respectively.

By analyzing Figure 4, we notice that as v exceeds $v_{min}^{\bar{S}}$ (the minimal value of v under it we obtain $\bar{S} = 0$), $\bar{R}$ starts to decrease considerably. During that interval, $\bar{S}$ and $\bar{F}$ are expected to increase quickly (As shown in Figure 1 for $\bar{F}$). After reaching a minimal value, the risk starts to slightly increase, as $\bar{S}$ and $\bar{F}$ cease to grow with the growth of v ($\bar{F}$ converges to an asymptotic value as shown in Figure 1) . We notice that for a completely vulnerable systems ($v = 1$), the expected risk of loss does not exceed 0.25, which represents 0.5% of L. In this analysis, we have also evaluated the impact of over and under investment in $\bar{S}$ on $\bar{R}$. We noticed that the impact is very low for low vulnerable systems, but increases with the increase of v. An over investment in $\bar{S}$ by 10% (which corresponds to the increase of $\bar{S}$ by 9.2×10^{-3} of L) contributes to the reduction of the optimal residual risk of loss by 0.02 (which represents 4.10^{-4} of L). The same proportions hold

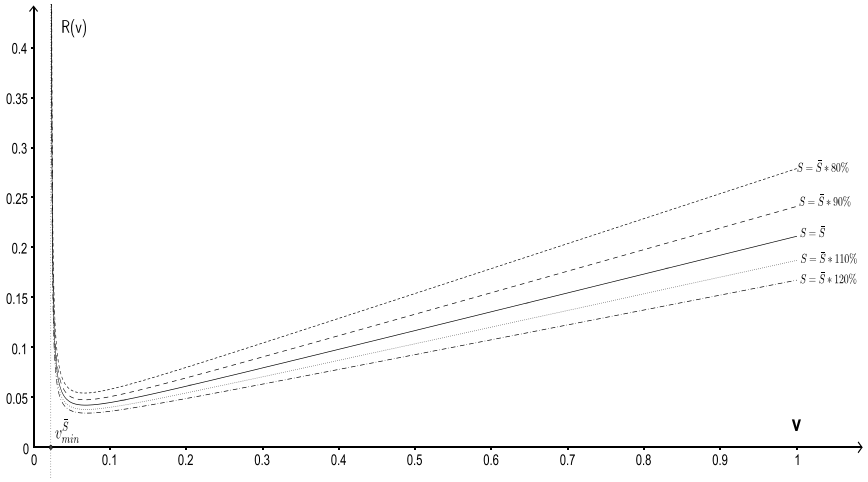


Figure 4: Residual Risk of Loss $\bar{R}$ with respect to Vulnerability rate v

for the remaining scenarios of over investments. The inverse statements are valid for the different scenarios of under investment. Even, if the cost-benefit of an over investment is not encouraging, the increase of Self Defense is always paying off to the firm, as it decreases the probability of loss and period of system downtime, and helps the firm sparing the time required to investigate a security breach, prepare the insurance claim, and wait for the reimbursement of the loss.

Analysis of the gained risk rate with respect to loss (for different vulnerability rates):
We examine in Figure 5, the rate of gained risk $\bar{G}$ by optimal investment in forensic readiness, with respect to potential loss (for different applied vulnerability rates). The rate $\bar{G}$ is defined as: $\bar{G} = (\mathring{R} - \bar{R})/\mathring{R}$, where $\mathring{R} = \bar{\phi} urL$ represents the risk of loss when no investment in forensic readiness is done (i.e., $\bar{F} = 0$). We obtain $\bar{G} = (\bar{\phi} urL - \bar{\phi}\bar{\rho}L(1-\lambda))/(\bar{\phi} urL)$. We notice that the gained risk increases with the increase of loss, for all values of v. As L increases, the value of $\bar{G}$ starts to increase considerably, and after that it starts to converge to an asymptotic value. This is due to the fact that $\bar{\phi}$ and $\bar{\rho}$ probabilities will decrease very slowly, when $\bar{F}$ and $\bar{S}$ start to converge to asymptotic values. By increasing v, the minimal value of loss L^v_{min} (upon which the gained risk starts to increase) increases. Therefore, by hardening the security of its assets to reduce the vulnerability rate, a firm would simply justify the need to not invest in lower values of L, but as long as L increases, the same rate of gained risk is observed for all systems whatever their initial vulnerability rate is. Finally, the reached value of the rate of gained risk (almost 80%) should highly motivate risk averse decision makers to invest in forensic readiness and insurance.

Summarizing the simulation findings
The numerical evaluations we have conducted in this section, showed the following findings: a) A risk averse decision maker does not invest in forensic readiness for very low vulnerable systems. A minimal threshold value of the vulnerability rate exists, which increases with the increase of reimbursement rate; b) For a high value of potential loss, the vulnerability rate does not have an impact on the optimal amount of investment; c) An over or under investment in forensic readiness does not have a great impact on the residual risk of loss, unless the secured system is highly vulnerable; and d) The risk of loss gained by an optimal investment in forensic readiness reaches

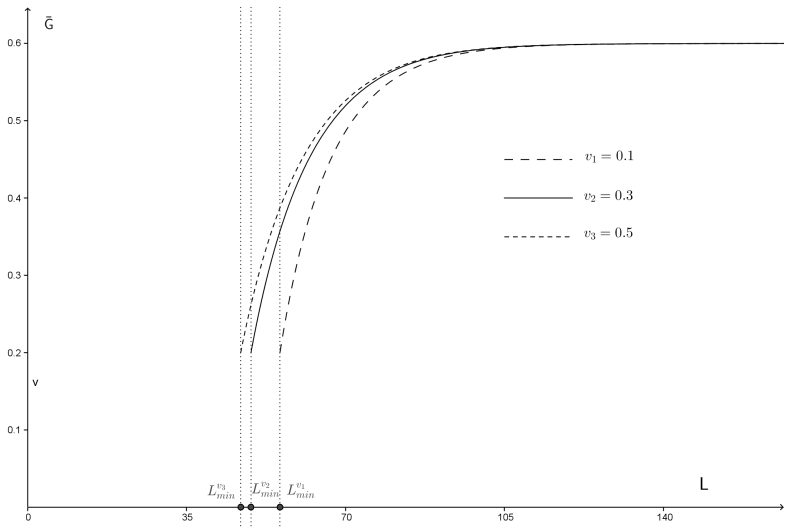


Figure 5: Rate of gained risk w.r.t Loss (L)

a maximal limit, if the potential loss becomes very important.

6 Conclusion

We introduced in this paper a new model and technique for the computation of optimal security investment, taking into consideration, in addition to the investment in self defense and insurance, the investment in forensic readiness to make incidents investigable. A new cyber security reimbursement policy which depends on the evidentiary aspects of the insurance claims, was proposed. Various analyses were conducted to estimate the optimal investment in self-defense and forensic readiness, and also the residual and gained risk.
In this paper, we separated the modeling and analysis of self-defense and forensics investment decisions. Developing in one model both of self-defense and forensics readiness investments, is an alternative solution, where a numerical resolution of the optimal investment equation would be required. It suffices to consider that the amount of a forensic readiness is proportional to the amount of a self-defense investment. In this work, we separate both types of investments, for the same of simplicity, as we believe that in practice an investor usually becomes convinced about an investment in forensic readiness after protecting his/her information system, assessing the residual risk, and financially assessing the insurance products available in the market.
As extension of this work will consider the use of game theory to integrate the strategic behavior of attackers, which could be threatened away by a big investment in forensic readiness, for example.

References

Bolot, Jean and Marc Lelarge (2008). "A New Perspective on Internet Security using Insurance." In: *Proceedings of the 27th Conference on Computer Communications*. AZ, USA.

Chandran, Rahul and Wei Q. Yan (2014). "Attack Graphs Analysis for Network Anti Forensics." *IGI Global International Journal of Digital Crime and Forensics (IJDCF)* 6 (1), 28–50.

Gordon, Lawrence A. and Martin P. Loeb (2002). "The economics of information security investment." *ACM Transactions on Information and Systems Security* 5 (4), 438–457.

Grossklags, Jens, Nicolas Christin, and John Chuang (2008). "Secure or Insure? A Game-Theoretic Analysis of Information Security Games." In: *Proceedings of the 17th International World Wide Web Conference*. Beijing, China.

Hausken, Kjell (2006). "Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability." *Information Systems Frontiers* 8 (5), 338–349.

— (2014). "Returns to information security investment: Endogenizing the expected loss." *Information Systems Frontiers* 16 (2), 329–336.

Huang, C. Derrick and Ravi S. Behara (2013). "Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints." *International Journal of Production Economics* 141 (1), 255–268.

Huang, C. Derrick, Qing Hu, and Ravi S. Behara (2008). "An economic analysis of the optimal information security investment in the case of a risk-averse firm." *International Journal of Production Economics* 114 (2), 793–804.

Ioannidis, Christos, David Pym, and Julian Williams (2013). "Economics of Information Security and Privacy III." In: ed. by Bruce Schneier. Springer New York. Chap. Fixed Costs, Investment Rigidities, and Risk Aversion in Information Security: A Utility-theoretic Approach, pp. 171–191.

Miaoui, Yosra, Noureddine Boudriga, and Ezzeddine Abaoub (2014). "Optimal Investment for Securing Enterprise Information Systems." In: *Proceedings of the 24th IBIMA Conference on Crafting Global Competitive Economies: 2020 Vision Strategic Planning & Smart Implementation*. Milan, Italy.

Ogut, Hulisi, Nirup Menon, and Srinivasan Raghunathan (2005). "Cyber Insurance and IT Security Investment: Impact of Interdependent Risk." In: *Proceedings of Fourth Workshop on the Economics of Information Security*. Cambridge, MA.

Pratt, John W. (1964). "Risk aversion in the small and in the large." *Econometrica* 32 (1-2), 122–136.

Sonnenreich, Wes (2006). "Return On Security Investment (ROSI) - A Practical Quantitative Mode." *Journal of Research and Practice in Information Technology* 38 (1), 45–56.

Wang, Jingguo, Aby Chaudhury, and H. Raghav Rao (2008). "A Value-at-Risk Approach to Information Security Investment." *Information Systems Research* 19 (1), 106–120.

Wang, Shyue Liang, Jyun Da Chen, Paul A. Stirpe, and Tzung-Pei Hong (2011). "Risk-neutral evaluation of information security investment on data centers." *Journal of Intelligent Information Systems* 36 (3), 329–345.

Willemson, Jan (2010). "Extending the Gordon and Loeb Model for Information Security Investment." In: *Proceedings of International Conference on Availability, Reliability, and Security*. Krakow, Poland.