Does Cyber-Insurance Benefit the Insured or the Attacker? – A Game of Cyber-Insurance

Zhen Li[1] and Qi Liao[2(✉)]

[1] Department of Economics and Management, Albion College, Albion, USA
zli@albion.edu
[2] Department of Computer Science, Central Michigan University, Mount Pleasant, USA
liao1q@cmich.edu

Abstract. Cyber-insurance is an insurance policy that protects the insured from a variety of cybersecurity incidents such as cyber-attacks, ransomware, and data breaches. The rapid expansion of cyber-insurance in recent years hints the strong demand for cyber-insurance and its benefits. However, the impacts of cyber-insurance practice on cybersecurity enhancement and cyber-attackers are largely unknown. In this paper we study the optimal cybersecurity investment and cyber-insurance decision-making systematically with special attention paid to the effects of the attacker's strategies. The economic modeling analysis and simulation study suggest that although cyber-insurance may be beneficial for the insured from a financial perspective, cyber-insurance practice may not be optimal from the societal cybersecurity perspective. Purchasing cyber-insurance decreases organizations' optimal cybersecurity investment and increases the attacker's expected payoffs. Therefore, the attacker has a motive to manipulate cyber-insurance by selective cyber-attacks on organizations up to a critical point, beyond which we discovered that imposing further threat will force organizations to invest more in cybersecurity. The attacker is capable of "playing god" by controlling the probabilities of initiating cyber-attacks and acts strategically to influence organizations' incentives to whether to purchase cyber-insurance to harvest benefits. This study of cyber-insurance' effects on attackers and their strategic manipulation of cyber-insurance provides insights for the future of the cyber-insurance market.

Keywords: cyber-insurance · cybersecurity investment · attacker manipulation · economic modeling and analysis · pricing · game theory

J. Fu et al. (Eds.): GameSec 2023, LNCS 14167, pp. 23–42, 2023.
https://doi.org/10.1007/978-3-031-50670-3_2

1 Introduction

Organizations in nearly every industry deal with cyber risk on a daily basis, and the financial devastation of cyber-attacks is only growing. The cybersecurity risks and incidents confronting organizations provide incentives for organizations to invest in cybersecurity. Since cyber-insurance became an option over a decade ago, the number of organizations purchasing cyber-insurance has been rising.

Cyber-insurance is an insurance policy that provides the insured with a combination of coverage options to protect the insured from losses due to a variety of cyber incidents such as data breaches, ransomware, denial-of-service attacks, etc. Coverage may include the liability of lost data, the damage to technology assets, the cost of business disruptions, informing affected clients, paying ransoms, and expenses and costs associated with legal issues. Like any insurance product, cyber-insurance pools the risks of cyber-attacks among policyholders. While cyber-insurance does not fundamentally change the overall destruction that a cybersecurity incident can cause, it reduces the organization's out-of-pocket payment ("private loss") in case of such an incident. In other words, cyber-insurance is to mitigate the organization's financial risk exposure in the aftermath.

Cyber-insurance is still in its early stage and its effects on cybersecurity remain an open question. Unlike the established insurances (e.g., home, auto, health, etc.) where the odds of incidents are more of "act of god" (e.g., a lightening hitting a house), in the new cyber-insurance, the odds of cyber-incidents are more controllable by the attacker. In some senses, the attacker's action is like the "hand of god" that controls the chance of cyber incidents. Therefore, this research focuses on the attacker's perspective and asks questions such as "Is cyber-insurance really good for cybersecurity?", "Can attackers benefit from the practice of cyber-insurance?", etc. By modelling a game between the attacker and the organization, we study the optimal strategies of both parties. Using a cybersecurity portfolio that consists of both cybersecurity investment (infrastructures, technologies, etc.) and cyber-insurance, we formulate an optimization problem to derive the optimal choice for the organization to choose between additional cybersecurity investment and purchasing cyber-insurance or not.

The novelty of this research is that it aims to study the possibility of the attacker's manipulation of cyber-insurance in their own favors by measuring the optimal cybersecurity investment level of the organization with and without cyber-insurance. A key determinant is the cyber threat imposed on the organization by the attacker. The attacker's action affects the organization's incentives to purchase cyber-insurance. Depending on how cyber-insurance may affect the attacker's benefits, the attacker strategically chooses attack probability imposed on the organization.

The modeling analysis and simulation study suggest a decrease in the organization's optimal cybersecurity investment with cyber-insurance, and there is a significant increase in the attacker's expected payoffs as the organization shifts from no cyber-insurance to cyber-insurance. Beyond that point of switch, imposing further threat on the organization will force the organization to invest more

in cybersecurity. In this scenario, the best response of the attacker is to impose just the right amount of cyber threat to "induce" the organization to purchase cyber-insurance. One of our important contributions is the finding of the critical point of attack probability for the organization switching to cyber-insurance therefore significantly increase attack payoff. To the best of our knowledge, this is the first study of the implications of cyber-insurance on the benefits of the attacker per se and the attacker's potential to manipulate the mechanism to serve their own best interests.

The rest of the paper is organized as follows. Section 2 reviews literatures on cyber-insurance. Section 3 conducts economic analysis on the organization's optimal cybersecurity investment with and without purchasing cyber-insurance, the organization's optimal cyber-insurance option, the effects of the organization's actions on the attacker, and the attacker's optimal strategy of launching attacks. Section 4 illustrates results from simulation study. Finally, Sect. 5 concludes our work and discusses future research.

2 Related Work

Compared to established lines of insurance services, cyber-insurance is at its early stage of development. Cyber-insurance is subject to not only general problems prevailing insurance markets like adverse selection and moral hazard [7], it is much more complicated and challenging than other lines of insurance. The cyber-insurance market is particularly complex as it has to tackle with challenges and obstacles prevailing in the insurance market such as the diversity of insurance coverage generating uncertainty and the moral hazard problem [22,32]. Without considering catastrophic scenarios, the vast majority of cyber risks are insurable and cyber-insurance can be profitable [12,19,21]. The insurers may offer not only cyber-insurance contracts but also risk management services [25]. Post-incident covering by cyber-insurance contracts is commonly seen [28]. It is generally agreed that cyber-insurance is effective at post-incident responses [18,25].

While cyber-insurance appears to be a viable method for cyber risk transfer, numerous problems with the insurability of cyber risks impede the development of the cyber-insurance market. Surveys and literature reviews classified researches on cyber-insurance into various areas, identified and categorized practical research problems and cyber-insurance challenges, provided the landscape and trends of the research and proposed possible solutions [1,6,28]. There are concerns about the insurance coverage, lack of information, and the complexity of the cyber-related claims [2]. Problems such as information asymmetries due to lack of data hinder cyber risk management via cyber-insurance [3,15]. A three-player game [27] implies attacks motivate the organizations to consider cyber-insurance option for transferring the risks. With malicious users present, equilibrium cyber-insurance contract that specifies user security fails to exist, and thus cyber-insurers fail to underwrite contracts conditioning the premiums on security in a general setting [8]. Recent empirical evidence suggests today's

cyber-insurance market is not effectively exercising predicted governance functions on cybersecurity [33].

The effects of cyber-insurance on cybersecurity investment is an open question. Cyber-insurance could result in higher cybersecurity investment depending on the insurers' ability to deal with potential adverse selection, moral hazard, and other problems in the cyber-insurance market [12]. An insurance contract incentivizing the insured to adopt preventative measures and implement best practices can improve cybersecurity provided by premium discrimination and the design of customized policies [11,13,30]. Security interdependence affects the incentive of users to invest in self-protection with and without cyber-insurance [29]. The key to improving overall network security lies in incentivizing users to invest in sufficient self-defense investments despite of the possible free-riding on others' investing in the network. Under conditions of no information asymmetry between the insurer and the insured, cyber-insurance incentivizes users to invest in self-defense [5,16].

Nevertheless, in a model where a user's probability to incur cyber damage depends on both private security and network security, competitive cyber-insurers may fail to improve network security [24]. Modeling the reactivity of the attacker to cybersecurity investment as an endogenous risk generating mechanism, it was shown that cyber-insurance may have negative effects on security investment [17]. Without contract discrimination, the cyber-insurance market equilibrium is inefficient and does not increase cybersecurity [13,14,20]. There is little empirical evidence that cyber-insurance gives motives for the insured to invest in cybersecurity [26,31]. A big challenge is the insurers' missing solid methodologies, standards, and tools to carry out their measurements [23]. A unifying framework was introduced considering interdependent security, correlated risk, and information asymmetries of cyber-insurance to understand the discrepancies [4]. A more recent study questions to what extent cyber-insurance companies influence global diffusion of cybersecurity protection and increase cybersecurity mechanisms [32]. To date, the cybersecurity implication of cyber-insurance remains a field of ambiguity.

Our research is related to existing literature on the incentive mechanisms of cyber-insurance but focuses on a novel angle. Based on the observation of cyber risk not being random and is largely in the control of the attacker, we have a particular interest in the attacker's attitude towards cyber-insurance, i.e., would the attacker welcome cyber-insurance? Since the attacker's likelihood of attack is a key determining factor of the organization's decision, the attacker can intentionally manipulate the whole system by adjusting their attack strategies in terms of attack probabilities to influence organizations' decision of purchasing cyber-insurance, thus benefit the most from the practice of cyber-insurance.

Shifting risks to the insurer or shifting liability on the insured to invest more is not enough for a successful cyber-insurance market. This paper considers a cybersecurity portfolio that consists of both optimal cybersecurity infrastructure investment and cyber-insurance purchase. By extending the Gordon-Loeb model [9,10], economic cost-benefit analysis determines the optimal amount of cyber-

security investment by taking into account the vulnerability of the organization to a security breach and its potential loss. Our model predicts the critical point (threshold) for the organization to shift from no insurance to insurance. Such a shift can benefit the attacker thus the attacker has the motive to push the organization to become insured. To generalize, no matter whether cyber-insurance has a positive or adverse overall effects on cybersecurity, the attacker can induce the organization to act in a way that is to the benefit of the attacker.

3 Game of Cyber-Insurance

There are two components of financial investment in cybersecurity portfolio: investment in fundamental cybersecurity infrastructure ("cybersecurity investment") and investment in cyber-insurance policy ("cyber-insurance"). The key difference between cybersecurity investment and cyber-insurance is that the former is preventive affecting the organization's fundamental vulnerability to cyber-attacks and the latter is aftermath coverage and clean-up, which by itself, does not affect the inherent vulnerability of the organization.

How much should the organization invest in cybersecurity? All in all, the organization is driven by the desire to earn profit, and its decisions are largely the result of cost-benefit analysis. We apply and extend economic production theory to the problem of assessing the impacts of cybersecurity investment and cyber-insurance. The production theory framework is based on the analysis of the relationship between cybersecurity inputs and output, or equivalently, costs and benefits. Table 1 lists the variables used in the model and their brief meanings.

Table 1. Symbols and Definitions

Symbol/Variable	Definition
C_s	cost of additional cybersecurity investment
C_i	cost of cyber-insurance (premium on cyber-insurance policy)
L_0	cyber incident loss without cyber-insurance
L_1	cyber incident loss with cyber-insurance (e.g., deductible)
t	attack probability
r	attack success rate at existing cybersecurity investment
$R(C_s, r)$	attack success rate with additional cybersecurity investment
P^a	attacker's payoff from a successful attack
C^a	attacker's cost of launching an attack

3.1 Inputs and Output of Cybersecurity Investment and Cyber-Insurance

We consider a one-period model of an organization contemplating a cybersecurity portfolio made up of cybersecurity investment and cyber-insurance. The organization is risk-neutral meaning that it is indifferent to amounts of investments or forms of investments as long as they have the same expected net value, regardless of various levels of risk and uncertainty.

Cybersecurity inputs include cybersecurity investment used to strengthen cybersecurity systems such as intrusion detection/prevention systems, firewalls, malware detection, antivirus and improved software, one time password tokens, two-factor authentications, encryptions, internal control systems, user education/training programs, etc. The organization's additional spending on cybersecurity investment is represented by C_s. In the context of cyber-insurance, cybersecurity inputs also include cyber-insurance policy premium, represented by C_i, had the organization chosen to purchase cyber-insurance.

Cybersecurity output is gauged by the reduced attack success rate generated by cybersecurity investment and the reduced incident loss private to the organization under the coverage of cyber-insurance. Following the Gordon-Loeb model [9], we measure the potential loss of cyber incident using triple variables $\{t, r, L_0\}$ where $t \in [0, 1]$ is the attack probability that the attacker may launch an attack on the organization, $r \in [0, 1]$ is the attack success rate at existing cybersecurity investment, and L_0 is the incident loss of a successful attack.

Specifically, the parameter r is used to denote the attack success rate at existing cybersecurity investment, the probability that without additional cybersecurity investment, a cyber attack will result in the organization's being victim of the attack and the loss L_0 occurring. Typically, the attack probability on the organization and the attack success rate would lie in the interior of $0 < t < 1$ and $0 < r < 1$. $t \times r \times L_0$ is the organization's expected loss conditioned on neither no additional cybersecurity investment nor cyber-insurance coverage. The organization's cybersecurity investment decision is on incremental investment spending, based on the implicit assumption that the organization already has some cybersecurity infrastructure in place, resulting in existing current attack success rate. Therefore, there are no incremental fixed costs associated with additional cybersecurity investment, only variable costs.

The expenditure of C_s is to reduce attack success rate r. Let $R(C_s, r)$ be the attack success rate on the organization that has additional investment amount of C_s. $R(C_s, r)$ is continuously twice differentiable. The nature of cyber vulnerability leads to the following features of the R function:

- $R(C_s, 0) = 0$ for all C_s. That is, if the organization is perfectly secure, then it will remain perfectly secure regardless of additional cybersecurity investment.
- $R(0, r) = r$ for all r. That is, if there is no additional cybersecurity investment, attack success rate remains unchanged.
- $R'(C_s, r) < 0$ and $R''(C_s, r) > 0$ for all $r \in (0, 1)$ where R' and R'' denote the first-order and second-order partial derivatives of the R function with

respect to C_s, respectively. That is, cybersecurity is increasing in cybersecurity investment at a decreasing rate.

The third feature of the R function implies that no finite cybersecurity investment can make the organization perfectly secure.

Cyber-insurance is specifically designed to address cyber-incident-related losses. Being insured does not reduce incident loss, but it may significantly decrease the organization's private loss in case of incident. The organization has to pay a premium to be insured. Due to moral hazard concerns, insurance policies normally come with deductibles. The premium and the deductible are the inputs of cyber-insurance.

Purchasing cyber-insurance does not change the incident loss L_0. Acquiring cyber-insurance does not increase or decrease the attack success rate, either. That is, r (and hence $R(C_s, r)$) is independent of C_i. The expenditure of C_i is to reduce the organization's private loss of incident. Suppose cyber-insurance reduces the organization's private loss from L_0 to L_1. L_1 includes the deductible and the part of incident loss not covered by cyber-insurance. It can also be extended to include the net present value of expected future increase in premiums.

The organization can affect the attack success rate via cybersecurity investment and expected private loss via cybersecurity investment and cyber-insurance, but the organization cannot invest to reduce attack probability. Hence attack probability t is exogenous to the organization, which is the control variable of the attacker. The organization decides on cybersecurity investment and cyber-insurance to reduce the expected net loss private to the organization.

3.2 Organization's Strategy

To determine the amount to invest in cybersecurity and cyber-insurance, the organization compares the expected benefits and expected costs of the two.

Choose Optimal Cybersecurity Investment Without Cyber-Insurance. For comparison, we begin with the case when cyber-insurance is not an option yet, i.e., $C_i \equiv 0$. The expected benefit of cybersecurity investment is equal to the reduction in the organization's expected loss attributed to additional cybersecurity investment.

$$[r - R(C_s, r)]tL_0 \tag{1}$$

Since C_s is the cost of cybersecurity investment, the expected net benefit of cybersecurity investment is

$$[r - R(C_s, r)]tL_0 - C_s \tag{2}$$

Of variables in (2), t is the control variable of the attacker. r and L_0 are the given parameters specifying the existing status of cybersecurity of the organization. C_s is the only control variable of the organization. The risk-neutral

organization's goal is to choose optimal additional cybersecurity investment C_s^* that maximizes (2).

C_s^* is found by solving the first-order condition of the objective function (2) with respect to C_s.

$$-R'(C_s^*, r)tL_0 = 1 \tag{3}$$

where the left-hand-side is the marginal benefit of cybersecurity investment measured by the decrease in attack success rate when increasing cybersecurity investment by one unit. This partial derivative can be interpreted as the marginal productivity of cybersecurity investment. The right-hand-side is the marginal cost of increasing cybersecurity investment by one unit.

Choose Optimal Cybersecurity Investment with Cyber-Insurance. When cyber-insurance is an option, the organization makes rational choice to determine if it needs cyber-insurance based on its own risk exposure. The insurer offers various combinations of premium and deductible to the organization, corresponding to the coverage and the attack success rate. In the one-period model, we assume the price of purchasing cyber-insurance depends on existing cybersecurity investment but not on the additional cybersecurity investment the organization will choose after purchasing cyber-insurance (which will affect future premium). Hence the organization's choice of cybersecurity investment (after being insured) does not affect the current premium, similar to a driver's current driving habits (after being insured) does not affect the current premium on the auto insurance policy.

The premium and the deductible are inversely related. The inverse relationship may apply to the following scenarios:

- The organization chooses a cyber-insurance policy that has a high deductible to reduce the premium, or a high premium to reduce the deductible.
- The organization pays a high premium on a cyber-insurance policy with broad coverage that reduces the organization's private loss in case of incident.

Cyber-insurance reduces the organization's private loss from L_0 to L_1. L_1 captures the deductible. Taking as given its chosen cyber-insurance package of $\{L_1, C_i\}$, the organization's expected benefit of additional cybersecurity investment with cyber-insurance is

$$[r - R(C_s, r)]tL_1 \tag{4}$$

The expected net benefit of additional cybersecurity investment with cyber-insurance is

$$[r - R(C_s, r)]tL_1 - C_s \tag{5}$$

The organization chooses optimal additional cybersecurity investment, C_s^{**}, to maximize (5):

$$-R'(C_s^{**}, r)tL_1 = 1 \tag{6}$$

Effects of Cyber-Insurance on Cybersecurity Investment. The optimal additional cybersecurity investment increases in attack probability as well as the organization's private loss.

From (3),

$$-R'(C_s^*, r) = \frac{1}{tL_0} \tag{7}$$

From (6),

$$-R'(C_s^{**}, r) = \frac{1}{tL_1} \tag{8}$$

If the organization were perfectly secure ($r = 0$), then no cybersecurity investment would be necessary ($C_s^* = C_s^{**} = 0$). At some sufficiently large attack success rate, it would be optimal to make positive additional cybersecurity investment.

Since R' is increasing in C_s and $L_0 > L_1$, optimal additional cybersecurity investment decreases when the organization has cyber-insurance coverage, i.e., $C_s^{**} < C_s^*$.

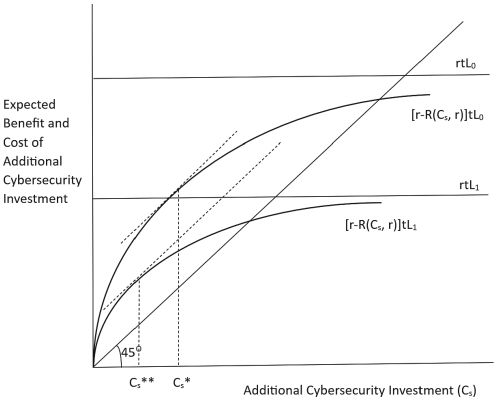


Fig. 1. Optimal additional cybersecurity investment with and without cyber-insurance.

Figure 1 illustrates the relative amounts of optimal additional cybersecurity investment. The horizontal axis is various levels of additional cybersecurity investment. The vertical axis measures expected benefits and costs of cybersecurity investment with and without cyber-insurance. The concave curves are for (1) and (4), respectively, of which, the lower curve is for (4). Both curves of expected benefits start from the origin at $R(0, r) = r$. They increase at a decreasing rate and converge to rtL_0 and rtL_1, respectively, as $C_s \to \infty$. The 45^o line is the cost curve of cybersecurity investment. The vertical distance between the concave benefit curve and the linear cost curve is the expected net benefit, as in (2) and (5), and the corresponding level of cybersecurity investment is the optimal. Note the intersection of the expected benefit curve and the cost curve corresponds to

the largest feasible additional cybersecurity investment. As long as cybersecurity investment stays below this amount, the organization's expected net benefit is positive. That is, it would receive a net benefit from additional cybersecurity investment. Nevertheless, the net benefit is maximized at an amount lower than the feasible upper-bound. As shown, the organization holding a cyber-insurance policy decreases additional cybersecurity investment.

The first-order conditions represented by (7) and (8) are applicable when the organization's optimal additional cybersecurity investment has an interior solution. In general, the organization chooses nonzero additional cybersecurity investment if and only if (2) or (5) is nonnegative. It is possible that the organization's optimal additional cybersecurity investment is zero in the following two scenarios.

- The organization is perfectly secure thus $R(C_s, 0) = 0$ for any C_s. Optimal additional cybersecurity investment is hence zero, the origin in Fig. 1.
- The organization's expected net benefit of additional cybersecurity investment is negative for any C_s, i.e., if the concave curve in Fig. 1 falls entirely below the 45^o cost line. This could be the case if the organization has little expected private loss (i.e., attack probability is small and private loss is small) and/or cybersecurity investment is ineffective at reducing attack success rate (i.e., $R(C_s, r)$ is high).

Since $L_1 < L_0$, the latter scenario is more likely to occur with cyber-insurance.

Choose Optimal Cyber-Insurance. The cost of cyber-insurance is C_i and the expected benefit of being insured is $R(C_s^{**}, r)t(L_0 - L_1)$. The organization decides on cyber-insurance purchase to maximize expected net benefit of cyber-insurance.

$$R(C_s^{**}, r)t(L_0 - L_1(C_i)) - C_i \tag{9}$$

Recall C_i and L_1 are inversely related and C_s^{**} depends on L_1. If L_1 is continuously differentiable in C_i and the optimal cyber-insurance has an interior solution, the optimal cyber-insurance premium C_i^* solves the first-order condition of (9). If L_1 is not continuously differentiable in C_i, which is more likely to be the case, the organization would choose the optimal insurance package $\{L_1^*, C_i^*\}$ from available discrete cyber-insurance packages that generates the largest expected net benefit, i.e., $R(C_s^{**}(L_1^*), r)t(L_0 - L_1^*) - C_i^* \geq R(C_s^{**}(L_1), r)t(L_0 - L_1) - C_i$ for all $\{L_1, C_i\}$.

It is possible that the organization's optimal cyber-insurance does not have an interior solution. In general, the organization would not purchase cyber-insurance if the expected net benefit of cyber-insurance (9) is not positive. The organization's optimal cyber-insurance is zero in the following two scenarios.

- The organization is perfectly secure thus $R(C_s^{**}(L_1), 0) = 0$ for any L_1.
- The organization's expected net benefit of cyber-insurance is negative for any $\{L_1, C_i\}$. This could be the case if the organization has little expected

incident loss (i.e., attack probability is small and incident loss is small) and/or the cyber-insurance policy offered is unfavorable.

3.3 Attacker's Strategy

The attacker launches cyber-attacks to maximize expected net payoff:

$$\max_t R(C_s(t), r)tP^a - tC^a \tag{10}$$

where P^a is the attacker's payoff received from a successful attack and C^a is the cost of attack. For simplicity, assume the game between the organization and the attacker is zero sum, i.e., $L_0 = P^a$. Given t, the attacker's highest possible expected net payoff is $R(0, r)tL_0 - C^a = rtL_0 - C^a$. This is the default benchmark of zero additional cybersecurity investment with and without cyber-insurance. As C_s increases, the attacker's expected net payoff decreases since $R(C_s, r)$ is decreasing in C_s.

Attacking the organization is profitable as long as $R(C_s(t), r)L_0 > C^a$. The parameters characterizing the organization's attractiveness to the attacker are $R(C_s, r)$ and L_0. Whether the organization buys cyber-insurance does not affect L_0 that is either paid by the organization, the insurer, or both. $R(C_s, r)$ increases as C_s decreases. The organization's purchasing cyber-insurance is beneficial to the attacker if the organization reduces additional cybersecurity investment when insured. Such potential gain for the attacker can only be realized if the organization chooses to buy cyber-insurance.

From (9), the organization chooses to buy cyber-insurance if it faces a high attack probability and there exists a cyber-insurance bundle that satisfies

$$t \geq \frac{C_i}{R(C_s^{**}, r)(L_0 - L_1)} \tag{11}$$

where the right-hand side is the lowest attack probability making the organization willingness to buy cyber-insurance, which is decreasing in L_0. It implies that compared to small and medium-sized organizations, large organizations with high incident loss are more likely to buy cyber-insurance.

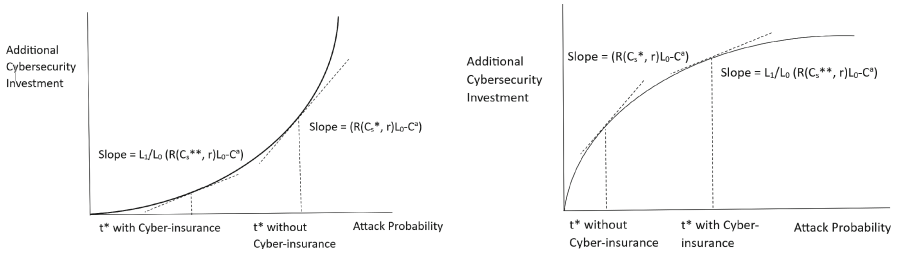
Buying cyber-insurance is beneficial for the organization when (11) holds true. Since t is a control variable of the attacker, the attacker can affect the organization's decision to buy cyber-insurance. When t increases, the organization is more likely to buy cyber-insurance, other things constant.

Nevertheless, other things are not constant. Although r and L_0 are exogenous and $\{L_1, C_i\}$ are predetermined, C_s increases with t, and hence R is decreasing in t. The attacker faces a tradeoff when raising the attack probability on the insured organization: an increase in t increases optimal additional cybersecurity investment, decreasing attack success rate and hence expected payoff while the increased t itself increases the expected payoff. The attacker has to control t strategically to generate a positive net gain.

With and without cyber-insurance, the attacker chooses t to solve (10). The first-order condition is

$$R'(C_s, r)\frac{dC_s}{dt}tL_0 + R(C_s, r)L_0 = C^a \tag{12}$$

Combined with (7) and (8), the attacker's optimal attack probability solves $\frac{dC_s^*}{dt} = R(C_s^*, r)L_0 - C^a$ without cyber-insurance, and $\frac{dC_s^{**}}{dt} = \frac{L_1}{L_0}(R(C_s^{**}, r)L_0 - C^a)$ with cyber-insurance.



(a) Case I: Additional cybersecurity investment is increasing in attack probability at an increasing rate

(b) Case II: Additional cybersecurity investment is increasing in attack probability at a decreasing rate

Fig. 2. The attacker's optimal attack probability with and without cyber-insurance, depending on the organization's choice of additional cybersecurity investment in response to attacker's attack probability.

$L_1 < L_0$, $C_s^* > C_s^{**}$ and $R(C_s^*, r) < R(C_s^{**}, r)$. The relative size of $\frac{dC_s^*}{dt}$ and $\frac{dC_s^{**}}{dt}$ depends. Facing the tradeoff, how cyber-insurance affects the attacker's optimal attack probability depends on how cybersecurity investment responds to attack probability. Suppose $(R(C_s^*, r)L_0 - R(C_s^{**}, r)L_1) > C^a(1 - \frac{L_1}{L_0})$, thus $\frac{dC_s^*}{dt} > \frac{dC_s^{**}}{dt}$. If cybersecurity investment is increasing in attack probability at an increasing rate (Fig. 2a), the attacker shall decrease the attack probability on the insured organization. If cybersecurity investment is increasing in attack probability at a decreasing rate (Fig. 2b), the attacker shall increase the attack probability on the insured organization. $\frac{dC_s}{dt}$ measures the slope of the cybersecurity investment curve. It would be the opposite if $\frac{dC_s^*}{dt} < \frac{dC_s^{**}}{dt}$.

In summary, if the attacker holds constant attack probability, the introduction of cyber-insurance benefits the attacker by decreasing the organization's additional cybersecurity investment. The attacker may increase attack probability to "induce" the organization to become insured. If the organization is already insured, the attacker needs to choose the optimal attack probability strategically to maximize the attack payoff. In practice, the attacker often lacks the knowledge of which organization is insured. Thus, Case II in Fig. 2 is in favor of the attacker as it justifies the consistent strategy of increasing the attack probability regardless of whether the organization is insured or not. As counteracts, the

organization shall consider the appropriate mechanism to adjust cybersecurity investment in response to the attacker's attack probability. It is also necessary to keep the purchase of cyber-insurance private information unreleased to the attacker.

4 Simulation Study

In this section, we conduct simulations to study the attacker's strategies and their impact on the organization's strategy of cybersecurity portfolio in terms of cybersecurity investment and cyber-insurance. In particular, we study the effects of attack probability on the organization's additional cybersecurity investment and on the attacker's expected payoffs with and without cyber-insurance.

The following function of attack success rate is used in simulations:

$$R(C_s, r) = \frac{r}{(\alpha C_s + 1)^{\beta}} \tag{13}$$

where $\alpha > 0$ and $\beta \geq 1$. $R(C_s, r)$ is decreasing in both α and β. Such a R function has a relatively simple functional form and satisfies all the three features the function shall have, as specified in Sect. 3.1. For illustration purpose and without loss of generality, we set the parameter values at $\alpha = 0.5$ and $\beta = 1.2$. The simulation results hold for all values of $\alpha > 0$ and $\beta \geq 1$.

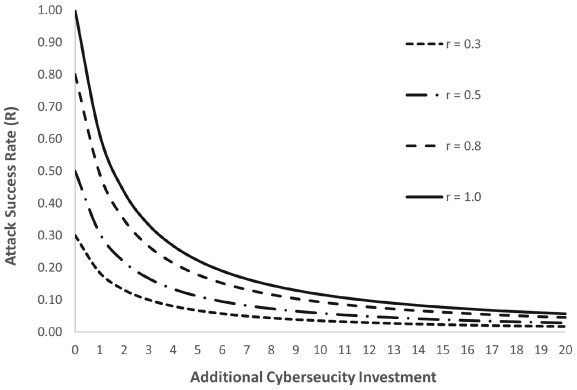


Fig. 3. Organization benefits from additional cybersecurity investment with decreasing attack success rate at a diminishing effect.

4.1 Attack Success Rate vs. Optimal Cybersecurity Investment with Cyber-Insurance

Figure 3 illustrates, given attack success rate at existing cybersecurity investment, how attack success rate changes with additional cybersecurity investment.

As shown, while attack success rate decreases with additional cybersecurity investment, additional cybersecurity investment cannot reduce attack success rate to zero. Recall r is the attack success rate at $C_s = 0$ and $R(0, r) = r$. Let additional cybersecurity investment ranges between 0 and 20, $R(C_s, r)$ decreases when C_s increases, calculated using (13). Unless the organization is perfectly secure that does not require additional cybersecurity investment ($r = 0$), the organization that is vulnerable to cyber-threat benefits from additional cybersecurity investment. However, the organization cannot be 100% secure with additional cybersecurity investment.

The marginal effect of cybersecurity investment can be found by solving for the partial derivative of (13) with respect to C_s,

$$R'(C_s, r) = -\beta\alpha r(\alpha C_s + 1)^{-1-\beta} \tag{14}$$

Combining (7) and (8) with (14), we find optimal additional cybersecurity investment without and with cyber-insurance.

$$C_s^* = \frac{(\alpha\beta r t L_0)^{\frac{1}{1+\beta}} - 1}{\alpha} \tag{15}$$

$$C_s^{**} = \frac{(\alpha\beta r t L_1)^{\frac{1}{1+\beta}} - 1}{\alpha} \tag{16}$$

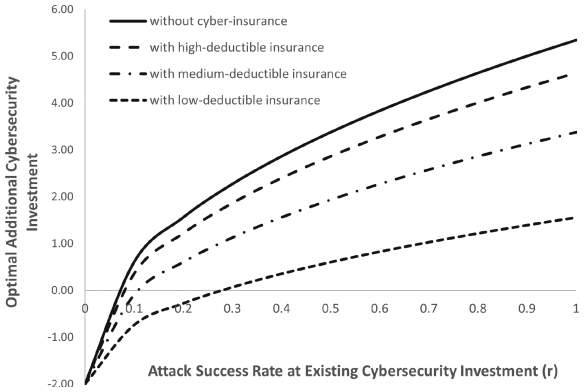


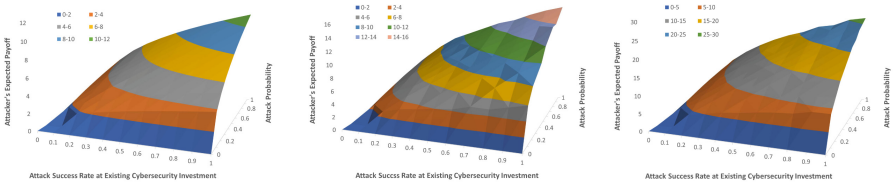
Fig. 4. While optimal additional cybersecurity investment (insured or not) increases when attack success rate (at existing cybersecurity investment) rises, cyber-insurance actually reduces optimal cybersecurity investment and increases the critical point (threshold) of cybersecurity investment. Organizations will not invest in additional cybersecurity below the critical point.

Figure 4 illustrates the organization's optimal additional cybersecurity investment given attack success rate at existing cybersecurity investment. Set $t = 0.3$

and $L_0 = 100$, three scenarios of private loss with cyber-insurance ($L_1 = 80$, $L_1 = 50$, and $L_1 = 20$) are considered. The horizontal axis measures attack success rate at existing cybersecurity investment. The vertical axis is the organization's optimal additional cybersecurity investment. The intersection of any curve and the horizontal axis is the *critical point* or *threshold* of attack success rate at existing cybersecurity investment that the organization would choose to invest more in cybersecurity.

The organization will not choose additional cybersecurity investment ($C_s = 0$) if the attack success rate is below the critical point. From (15) and (16), the optimal additional cybersecurity investment equals zero until $r = \frac{1}{\alpha\beta t L_0}$ without cyber-insurance and $r = \frac{1}{\alpha\beta t L_1}$ with cyber-insurance. At the specified parameters, the former is 0.056 and the latter is 0.07, 0.11 and 0.28, at $L_1 = 80$, $L_1 = 50$, and $L_1 = 20$, respectively. As private loss decreases, the organization's willingness to invest in cybersecurity decreases.

Key observations from Fig. 4 include: 1) As attack success rate increases, optimal additional cybersecurity investment increases, insured or not; 2) Being insured decreases optimal additional cybersecurity investment. The decrease is increasing in the coverage of cyber-insurance; 3) Being insured increases the critical point (threshold) of additional cybersecurity investment. The threshold is increasing in the coverage of cyber-insurance.



(a) Without Cyber-Insurance (b) With High-deductible Cyber-insurance (c) With Low-Deductible Cyber-insurance

Fig. 5. The attacker's expected payoff grows from having no cyber-insurance (a) to having cyber-insurance (b and c)

4.2 Attacker's Expected Net Payoff

To study the effects of cyber-insurance on the attacker's expected payoff, we adopt a simplified "high deductible + low premium" + "low deductible + high premium" pricing model: Policy A with a bundle of $\{L_1 = 50, C_i = 3\}$ and Policy B with a bundle of $\{L_1 = 20, C_i = 7\}$. Figure 5 compares the attacker's expected payoff in three scenarios: without cyber-insurance, with cyber-insurance of high deductible (Policy A) and with cyber-insurance of low deductible (Policy B). The attacker's cost function is largely composed of fixed or sunk cost in acquiring knowledge and malware to launch attacks. The additional cost occurred on

attacking one more target is small. Moreover, the fixed cost of attack is the same with and without cyber-insurance. It is canceled out for comparison purpose. As shown in the figure, the peak payoff increases from range 10–12 (5a) to range 14–16 (5b), then to range 25–30 (5c). The results suggest that the attacker benefits from the organization's purchasing cyber-insurance and benefits further if the organization chooses cyber-insurance with low deductible.

4.3 Attack Strategy

For cyber-insurance, the organization chooses to purchase a policy bundle $\{L_1, C_i\}$ if

$$R(C_s^{**}, r)t(L_0 - L_1) \geq C_i \tag{17}$$

From (13),

$$R(C_s^{**}, r) = \frac{r}{(\alpha C_s^{**} + 1)^{\beta}} \tag{18}$$

Combined with (16),

$$R(C_s^{**}, r) = \frac{r}{(\alpha\beta r t L_1)^{\frac{\beta}{1+\beta}}} \tag{19}$$

Combined with (17), we can find that an insurance policy $\{L_1, C_i\}$ is beneficial to the organization facing attack probability

$$t \geq \{\frac{C_i(\alpha\beta r L_1)^{\frac{\beta}{1+\beta}}}{r(L_0 - L_1)}\}^{1+\beta} \tag{20}$$

where the right-hand side is the critical point (threshold) that the attacker may choose to trigger the organization to buy cyber-insurance.

Note (20) also provides insights on the role of parameters' configuration on organization's choice of cyber insurance and the attacker's best response. The condition would fail when the right-hand term is larger than one that could occur at $C_i(\alpha\beta r L_1)^{\frac{\beta}{1+\beta}} > r(L_0 - L_1)$, in which case, the organization would not choose cyber insurance regardless of the attacker's strategy. The cyber-insurance-policy specifications $\{L_1, C_i\}$ are among the key variables determining the value of the right-hand term. In a way, the attacker and the insurer may have aligned interests to make the organization choose cyber insurance, hence the efforts of insurance companies to promote cyber insurance can serve the purposes of cyber attackers.

Figure 6 shows the critical point (threshold) of attack probability at various attack success rate at existing cybersecurity investment and various available cyber-insurance policy options. The organization will not buy cyber-insurance if the attack probability is below the threshold. The threshold attack probability decreases if the organization is more vulnerable to cyber attacks (higher attack success rate). In the case the calculated threshold attack probability is above 1, the organization does not buy cyber-insurance regardless.

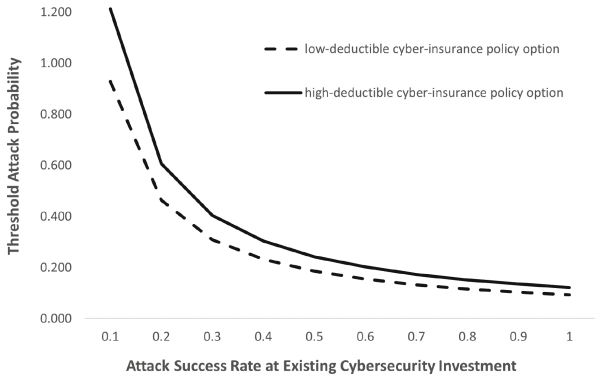
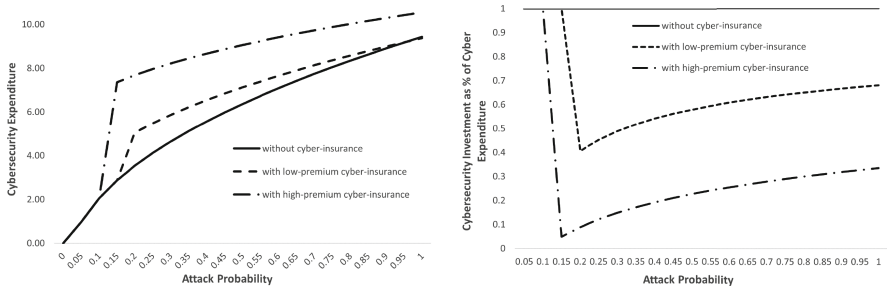


Fig. 6. If the attack probability is below the critical point (threshold), the organization will not buy cyber-insurance. The attacker may strategically choose an attack probability that will trigger the organization to buy cyber-insurance that benefits the attacker.



(a) Total cybersecurity expenditure rises sharply at the critical point

(b) Share of cybersecurity investment drops sharply at the critical point

Fig. 7. Manipulating attack probabilities may significantly increase organization's total cybersecurity expenditure through purchasing cyber-insurance at the critical point. The share of cybersecurity investment may also be decreased significantly at the critical point of attack probability due to purchasing cyber-insurance and bounces back gradually after being insured.

4.4 Cybersecurity Portfolio

Lastly, we simulate how the organization's cybersecurity portfolio in terms of total expenditure on both cybersecurity investment and cyber-insurance is affected by the attacker's actions. Without cyber-insurance, the organization's spending on cybersecurity investment is C_s^* as in (15). When the organization buys cyber-insurance, its total expenditure is $C_s^{**} + C_i^*$.

Figure 7a illustrates how the organization's total cybersecurity expenditure changes with attack probability. Total cybersecurity expenditure increases regardless, indicating an increased spending on cybersecurity when the organization faces increased attack probability. At the parameters used in the simulations,

especially the significant premium compared to optimal additional cybersecurity investment, total cybersecurity expenditure increases sharply at the critical point after buying cyber-insurance.

Figure 7b is cybersecurity investment as a fraction of the total expenditure. The share of cybersecurity investment falls sharply at the critical point when the organization buys cyber-insurance and the share bounces back as the organization increases cybersecurity investment at increasing attack probability. Empowered with the critical point (threshold), the attacker may manipulate attack probability to trigger the organization to buy cyber-insurance thus significantly increase the attacker's expected payoffs.

5 Conclusion

While more and more organizations adopt cyber-insurance, the effects of cyber-insurance on cybersecurity remains unclear. This research study focuses on a novel angle and sheds light on the overlooked issue of the effects of cyber-insurance from the attacker's perspective, and studies whether the attacker may manipulate and ultimately benefit from the cyber-insurance practice. Our research models a game between the attacker, whose strategy is to control attack probability, and the organization, whose strategy is to choose optimal cybersecurity portfolio consisting of both cybersecurity investment and cyber-insurance. The economic modeling analysis and simulation study suggest that although cyber-insurance may be beneficial for the insured organization from a financial perspective, cyber-insurance may not always be the best from the cybersecurity perspective. Especially, the attacker may benefit from cyber-insurance with higher expected payoff from increased attack success rate resulting from the organization's reduced optimal security investment. This paper contributes further by identifying the critical point (threshold) of such attack probability for organizations to switch to cyber-insurance practice, therefore significantly increase the cyber attack payoffs. In the future we plan to focus on the extension and the application of the model. For example, the details of cyber insurance policies will be explored by relating the premiums and deductibles to the risks. Self insurance may be included as an alternative in addition to prevention/mitigation and market insurance. Our future work will also study how the development of the cyber-insurance market shall take into account the implications of the market to the attacker and the counteracts to prevent the possible manipulation of the market by the attacker.

References

1. Aziz, B.: A systematic literature review of cyber insurance challenges. In: Proceedings of International Conference on Information Technology Systems and Innovation (ICITSI), Bandung, Indonesia, pp. 357–363 (2020)
2. Bandyopadhyay, T., Mookerjee, V.: A model to analyze the challenge of using cyber insurance. Inf. Syst. Front. **21**, 301–325 (2019)

3. Bandyopadhyay, T., Mookerjee, V.S., Rao, R.C.: Why IT managers don't go for cyber-insurance products. Commun. ACM **52**(11), 68–73 (2009)
4. Böhme, R., Schwartz, G.: Modeling cyber-insurance: towards a unifying framework. In: Proceedings of the 9th Workshop on the Economics of Information Security (WEIS), Cambridge, MA (2010)
5. Bolot, J.C., Lelarge, M.: Cyber insurance as an incentive for internet security. In: Proceedings of Workshop on the Economics of Information Security (WEIS), Hanover, NH, pp. 269–290 (2008)
6. Dambra, S., Bilge, L., Balzarotti, D.: SoK: cyber insurance - technical challenges and a system security roadmap. In: Proceedings of IEEE Symposium on Security and Privacy (SP), San Francisco, CA, pp. 1367–1383 (2020)
7. Ehrlich, I., Becker, G.S.: Market insurance, self-insurance, and self-protection. J. Polit. Econ. **80**(4), 623–648 (1972)
8. Schwartz, G., Shetty, N., Walrand, J.: Why cyber-insurance contracts fail to reflect cyber-risks. In: Proceedings of 51st Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, pp. 781–787 (2013)
9. Gordon, L.A., Loeb, M.P.: The economics of information security investment. ACM Trans. Inf. Syst. Secur. **5**(4), 438–457 (2002)
10. Gordon, L.A., Loeb, M.P., Lucyshyn, W., Zhou, L.: Increasing cybersecurity investments in private sector firms. J. Cybersecur. **1**(1), 3–17 (2015)
11. Hayel, Y., Zhu, Q.: Attack-aware cyber insurance for risk sharing in computer networks. In: Proceedings of the sixth International Conference on Decision and Game Theory for Security (GameSec), London, UK, pp. 22–34 (2015)
12. Kesan, J.P., Majuca, R.P., Yurcik, W.: Cyber-insurance as a market-based solution to the problem of cybersecurity. In: Proceedings of the 4th Workshop on the Economics of Information Security (WEIS), Cambridge, MA (2005)
13. Khalili, M.M., Naghizadeh, P., Liu, M.: Designing cyber insurance policies: the role of pre-screening and security interdependence. IEEE Trans. Inf. Forensics Secur. **13**(9), 2226–2239 (2018)
14. Khalili, M.M., Zhang, X., Liu, M.: Effective premium discrimination for designing cyber insurance policies with rare losses. In: Proceedings of the 10th International Conference on Decision and Game Theory for Security (GameSec), Stockholm, Sweden, pp. 259–275 (2019)
15. Laszka, A., Panaousis, E., Grossklags, J.: Cyber-insurance as a signaling game: self-reporting and external security audits. In: Proceedings of the 9th Conference on Decision and Game Theory for Security (GameSec), Seattle, WA, pp. 508–520 (2018)
16. Lelarge, M., Bolot, J.C.: Economic incentives to increase security in the internet: the case for insurance. In: Proceedings of IEEE International Conference on Computer Communications (INFOCOM), Rio de Janeiro, Brazil, pp. 1494–1502 (2009)
17. Massaccia, F., Swierzbinskic, J., Williams, J.: Cyberinsurance and public policy: self-protection and insurance with endogenous adversaries. In: Proceedings of 16th Annual Workshop on the Economics of Information Security (WEIS), La Jolla, CA, pp. 1–38 (2017)
18. Nurse, J.R., Axon, L., Erola, A., Agrafiotis, I., Goldsmith, M., Creese, S.: The data that drives cyber insurance: a study into the underwriting and claims processes. In: Proceedings of 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, pp. 1–8. (2020)
19. Pal, R., Golubchik, L., Psounis, K.: Aegis - a novel cyber-insurance model. In: Proceedings of Conference on Decision and Game Theory for Security (GameSec), College Park, Maryland, pp. 131–150 (2011)

20. Pal, R., Golubchik, L., Psounis, K., Hui, P.: Will cyber-insurance improve network security? A market analysis. In: Proceedings of IEEE Conference on Computer Communications (INFOCOM), Toronto, Canada, pp. 235–243 (2014)
21. Pal, R., Golubchik, L., Psounis, K., Hui, P.: The technologization of insurance: an empirical analysis of big data and artificial intelligence's impact on cybersecurity and privacy. ACM SIGMETRICS Perform. Eval. Rev. **45**(4), 7–15 (2018)
22. Panda, S., Woods, D.W., Laszka, A., Fielder, A., Panaousis, E.: Post-incident audits on cyber insurance discounts. Comput. Secur. **87**, 101593 (2019)
23. Romanosky, S., Ablon, L., Kuehn, A., Jones, T.: Content analysis of cyber insurance policies: how do carriers price cyber risk? J. Cybersecur. **5**(1), 1–19 (2019)
24. Shetty, N., Schwartz, G., Walrand, J.: Can competitive insurers improve network security? In: Proceedings of the Third International Conference on Trust and Trustworthy Computing (TRUST), Berlin, Germany, pp. 308–322 (2010)
25. Talesh, S.A.: Data breach, privacy, and cyber insurance: how insurance companies act as "compliance managers" for businesses. Law Soc. Inquiry **43**(2), 417–440 (2018)
26. Talesh, S.A., Cunningham, B.: The technologization of insurance: an empirical analysis of big data and artificial intelligence's impact on cybersecurity and privacy. Utah Law Rev. **2021**(5), 967–1027 (2021)
27. Tosh, D.K., et al.: Three layer game theoretic decision framework for cyber-investment and cyber-insurance. In: Proceedings of the 8th International Conference on Decision and Game Theory for Security (GameSec), Vienna, Austria, pp. 519–532 (2017)
28. Tsohou, A., Diamantopoulou, V., Gritzalis, S., Lambrinoudakis, C.: Cyber insurance: state of the art, trends and future directions. Int. J. Inf. Secur. 1–12 (2023)
29. Uuganbayar, G., Yautsiukhin, A., Martinelli, F.: Cyber insurance and security interdependence: friends or foes? In: Proceedings of 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA), Glasgow, UK, pp. 1–4 (2018)
30. Uuganbayar, G., Yautsiukhin, A., Martinelli, F., Massacci, F.: Optimisation of cyber insurance coverage with selection of cost effective security controls. Comput. Secur. **101**(102121), 1–21 (2021)
31. Wolff, J.: Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks. The MIT Press, Cambridge (2022)
32. Woods, D.W., Böhme, R.: How cyber insurance shapes incident response: a mixed methods study. In: Proceedings of the 20th Annual Workshop on the Economics of Information Security (WEIS), pp. 1–35 (2021)
33. Woods, D.W., Moore, T.: Does insurance have a future in governing cybersecurity? IEEE Secur. Priv. **18**(1), 21–27 (2020)