Cyber Insurance and Time-to-Compromise: An Integrated Approach

Ganbayar Uuganbayar[1,2], Fabio Massacci[2], Artsiom Yautsiukhin[1], and Fabio Martinelli[1]

[1]Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, Pisa, Italy,,
Email: {ganbayar.uuganbayar, artsiom.yautsiukhin, fabio.martinelli}@iit.cnr.it

[2]Department of Information and Communication Technology, University of Trento, Italy,,
Email: {ganbayar.uuganbayar, fabio.massacci}@unitn.it

***Abstract*—Fast-growing numbers of technologies and devices make cyber security landscape more complicated and require a more accurate models. This complexity challenges cyber security experts to devise a better solution to manage cyber risks. One of the promising methods is to find the best distribution of security expenditure for risk mitigation and transfer (i.e. cyber insurance) options.**

In this work, we propose a solution to find the optimal security investments when there is a cyber insurance option by applying time to compromise metric to the probability of attack computation. In particular, we find the best set of countermeasures which decreases the maximum number of vulnerabilities to increase the required time to compromise a system. Our approach is based on a multiple-objective knapsack problem for the selection of countermeasures and we find the best distribution of security expenditure by computing both probability of attack and time to compromise metric.

***Index Terms*—cyber insurance, security investment, time to compromise, risk management**

I. Introduction

It is expected that some of the current jobs will allegedly disappear in a near future due to the advanced technologies i.e. artificial intelligence. With the increase of technologies, we also witness the demand for cyber security experts in our daily life to deal with cyber-related risks. At the same time, managing cyber risks is one of the challenging tasks, where it commonly comprises risk assessment and treatment processes. So far, several security standards, guidelines and frameworks, such as NIST and ISO/SEC 27001, have been introduced and applied to organizations depending on their structure. However, we are still lacking in either theoretical model or practical solution, which has been confirmed by recent cyber attacks, i.e. ransomware attack hit over 150 countries in 2017 [1] and IoT oriented attacks increased by 600% in 2017 compared to 2016, while the increase in mobile malware was 54% [2]. Moreover, in recent years, the attack surface is changing with the increase of new technologies, such IoT and Cloud systems, where attackers are more capable to find the vulnerability to exploit [2], [3]. In order to face these challenges around us and potential threats, there is a need for an efficient and applicable solution, in terms of managing the cyber risks.

This work was partially supported by projects H2020 MSCA NeCS 675320 and H2020 MSCA CyberSure 734815.

To harden the cyber security management, risk treatment techniques, in particular, most of the guidelines and standards propose the following steps; (i) mitigate the cyber risk, (ii) transfer the risk to the third party, (iii) withdraw the risky part from a system or accept the risk. The last options, withdrawing and accepting the risk, are neglected in most theoretical cases. Cyber risk mitigation does not suffice the needs of an organization to protect the assets since there is always a residual risk although we are confident in our security [4]. Therefore, cyber insurance, a representative of cyber risk transfer, has been introduced, and where an organization pays premium[1] in return of the cover for the loss. This combination perspective of economic and hardware aspects was captured by Anderson et al. [5], indicating that cyber security economic is as crucial as installing countermeasures.

In the last years, cyber insurance has been bringing a positive effect on cyber security standards and to the economic point of view. Also its market is growing and its annual premium is expected to reach 14 billion (USD) in 2020, 28% greater than it was in 2016 globally [6]. On the other side, cyber insurance field is facing some challenges, i.e. interoperability of cyber insurance and security investments. Some researchers, such as Anderson et al. [7] advocates that cyber insurance incentivises organization (formal terminology is insured) to invest for the self-protection. With investing for ex-anti security, an organization is offered less premium by an insurer. On the contrary, some, [8]–[10], claim that cyber security investments is neglected due to the appearance of cyber insurance option since the insurer covers all the loss of insured if an incident occurs. It is worth noting that these different outcomes are based on various assumptions, i.e. cyber insurance market type - competitive or non-competitive insurance markets. Also, this dilemma comes from a consideration of different security investments models, continuous and discrete. The continuous investments model allows the probability of attack decreases with every security investments that an organization puts [8], [11], [12], while not every security investments leads to a low probability of attack, i.e. it can be seen as a futile countermeasure installation. There are many cyber insurance models that consider the former investments model as opposed to models by some researchers

[1]a fee from organization to insurance company

[13], [14], which considered the discrete investments model yet an oversimplified. In this work, we follow the former condition, cyber insurance encourages insured to invest, and look forward to the best distribution of security expenditure between cyber insurance and security investments.

In cyber insurance, the risk assessment is the base part to estimate the premium. In most cases, the premium is computed in an unfair way due to the lack of model or practical solution for computing the probability of attack. One of the solutions to capture this probability of attack is to consider the required time to compromise a system. We assume that the visibility of unknown vulnerabilities in the system increases with increase of time. With addressing this issue, defining this required time is the key to find the probability of attack and offer a fair premium to the organization.

In this work, we contribute an initial pace of introducing time to compromise metric to cyber insurance model to make it more dynamic. Our contribution consists of several simplifying assumptions yet is allowing us to enable a new approach. We compute the probability of attack and time to compromise metric based on vulnerabilities of a system, which is affected by the optimal security investments. Finally, we find the best security expenditure between risk mitigation and transfer techniques based on a multi-objective knapsack problem which is an extension of our last work [15]. The difference is that we consider the vulnerabilities in the system and embedded the time to compromise the metric to our algorithm. We particularly highlight that defining and applying time to compromise metric to cyber insurance model will lead us to a more promising solution which captures the dynamicity of the surrounding cyber environment by offering different cyber insurance policies to insureds in terms of the duration.

The remainder of this paper unfolds as follows. In the next section, we review existing models and literature related to our work (*Section II*). In *Section III*, we specify the problems that we will solve with the proposed solution (*Section IV*). The discussion and future works are illustrated in *Section V* and we conclude the work in *Section VI*.

II. Related work

According to some reports [6], [16], global cyber insurance market is expected to grow in 2022 up to 14 billion in terms of annual premium. Also, the impact of cyber insurance has been scientifically studied in several papers [11], [17]–[19] where the most of them proposed a theoretical work. Regardless of its market growth and a positive impact on security standards [3], [20], it faces some challenges i.e. security interdependence[2] and unfair premium estimation. In particular, form the perspective of insured, there is a need for knowing whether cyber insurance encourages organizations to invest in their ex-ante security controls (countermeasures) [8], [9], [12], [14], [21]. Many researchers support the idea that the availability of insurance incentivises the insured to invest more [7], [22], [23], while some [8]–[10] claim that, with certain considerations, an insured simply neglects the security investments and instead rely on only cyber insurance option. One of the central assumptions is that these works [8], [11]–[14], [24] are illustrated in two different insurance markets that affect the outcome significantly, competitive and non-competitive, respectively. Although the competitive market is a naive model [25] and is non-profit without any regulation, G.A.Schwartz et al. [10] and others [13] came up with a conclusion that cyber insurance could be an incentive for security investments if there is no information asymmetry[3]. On the other hand, an opposite conclusion that cyber insurance has a negative impact on the security investments was highlighted by H.Ogut et al. [8]. The discrepancy of these works is the security investments model where H.Ogut et al. [8] considered continuous model and Z.Yang et al. [13] evaluated the discrete investments model. Also, to model non-competitive markets, H.Ogut et al. [8] and others [26] introduced their work in the non-competitive insurance market where insurers are able to add an additional amount of fee, so-called loading factor. Similar to other [10], [13], [25], we conceptualize our solution in a competitive insurance market.

Cyber insurance formalizations have two types of security investments models; continuous and discrete security investments model [8], [11]–[14], [24]. In the continuous model, the probability of attack decreases with any additional security investments, while the probability of attack could be the same with different investments level after a certain point in the discrete investments model. The continuous model can be seen as an ideal model [8], [11], [12], where one cannot know how much organization should invest in order to improve the security and select the best controls. On the other hand, the discrete security investments model can be adapted in more practical cases and it has been investigated in some papers, such as [13], [14], where the authors considered an oversimplified model which neither computes the probability of attack nor improves the security in overall. In this work, we consider a case that insurance encourages the insured to invest, and the discrete security investments model where we show the dependency of countermeasures, risk assessment and cyber insurance premium.

Risk analysis and assessment is the fundamental necessity of cyber insurance and is required for the premium estimation [3]. However, assessment of cyber risks is more complicated due to the evolution of attack surface (i.e., cloud), fast-growing novel threats, lack of empirical data, and too generic models. The emerging technologies, cloud or IoT, are changing the cyber risk landscape rapidly [3], [20]. Also, the evolution of attack, performed by highly adaptable and unpredictable attackers, is another source of volatility [2], [27]. Cyber insurers have not yet fully determined/assessed which standards concretely affect an organization's security level as it is done in other areas of insurance [20], [28]. Moreover, the probability of attack a system is correlated with the required to compromise

[2] one's level of security depends on its neighbour's security investments as well

[3] it occurs when an insurer has no information about insured's security level

the system. In this regard, a required time-to-compromise metric for IT system has been investigated by some researchers [29]–[31]. In particular, some authors, i.e. [30], [31], highlighted that defining the time-to-compromise metric provides us with a reasonable metric to measure the security level of organizations. B.Littlewood et al. [29], advocate the idea quantitatively measuring the security of the system based on the analogy between its failure and security breach. Yet this work just described possible ways to measure the security and presented a pilot experiment. Some real case works have also been conducted in this issue, such as, A.Miles et al. (2006) [30] proposed the time-to-compromise model, that we adopted in this work, to reduce the cyber risk, which was applied to a SCADA system. However, the authors assumed the assumption that a system component is visible to an attacker and the model does not address the dependency between vulnerabilities on different system components. In particular, this model depends on an attacker's skill level and the vulnerability of the system and considers three phases for breaching the system. Also, a recent work by F.Massacci et al. [32] presented a model to estimate organization's probability of attack quantitatively, which is based on actual data that is accumulated through Intrusion Detection System (IDS) and periodic Vulnerability Assessment (VA). Since we should consider both defenders and attackers to have better security, there is a need to study the behaviour of attackers. To that end, the amount of time required for the attackers to take down the system has been investigated by D.John et al. (2009) [33]. What differs this work from others is that the authors incorporated the method of M.McQueen [30] into the attack tree approaches so that they are able to find the shortest path based on its required time. Similarly, W.Nzoukou et al. (2013) [34] proposed a framework for measuring the security of a network. The authors enhanced the idea presented by the D.John et al. [33] by adding the CVSS (Common Vulnerability Scoring System). It is worth noting that the vulnerabilities are mitigated by the selection of countermeasures and security investments that an organization puts on.

The selection process of the best countermeasures has been introduced in several papers [35], [37] and it is not a new issue. For instance, a capability of blocking a threat and the cost of countermeasure are considered in a model by T. Sawik [36], and he applies the conditional value-at-risk approach in harmony with single-or-bi-objective mixed integer program. In an optimisation problem, there are various types of solutions including knapsack problems [38]. To give an example, to find the optimal security investments, F. Smeraldi et. al. [35] introduced a framework which combines combinatorial optimisation with classical knapsack problem. One of the uses of the knapsack problem was introduced by L. Krautsevich et. al. [39] to select the most secure web services. As opposed to these papers, we considered different assumptions where our solution starts with an initial security investments and no limit to reach, applying a multi-objective knapsack problem. We also took into account that the countermeasure's efficacy is estimated by its capability of decreasing the number of vulnerabilities in a system. Finally, we did not simply apply the knapsack problem to our work, but we have also solved an issue of finding the optimal distribution of security expenditure and defining the relation between this selection process of countermeasures and the time-to-compromise metric.

III. Problem specification

Let us assume a situation where an organization i would like to protect its valuable assets against potential cyber attacks. In particular, there is a need for the best solution to distribute the security investments for risk mitigation (i.e. installing security controls) and transfer (e.g. cyber insurance) options to maximize the benefit within a certain T time. Organization i starts with an initial wealth W_i^0 and it expects the amount of wealth W_i after a certain period T. Let p_i be the probability of attack if an incident occurs and it depends on the time to compromise the organization t, $(t \leq T)$. We denote x_i as the security investments that an organization puts in its self-protection which affects both probability of attack p_i and time to compromise t, and our probability of attack the system is given as $p_i(t(x))$ that is equal to $p_i(x)$ (we use this version of probability hereinafter in this paper). Naturally, the probability of attack decreases with the increase of security investments $(\forall x_1 < x_2\ (p_i(x_1) > p_i(x_2))$ and also time to compromise t increases with the rise of security investments x_i. Eventually, if an attacker succeeds with $p_i(x_i)$, there is a loss, presented as L_i, to an organization which is consider as a single incident. On the other hand, we denote $\bar{V}_i = \langle V^1, V^2, ..., V^{n_y} \rangle$ as a number of vulnerabilities in the organization and each vulnerability triggers different losses in period T. In this regard, our probability of attack becomes a vector indicated by $\bar{p}_i(x_i) = \langle p_1(x_i),\ p_2(x_i), ...,\ p_{n_y}(x_i) \rangle$, and all vectors in this paper are of size n_y. We use different types of multiplying operation in our work, i.e. a usual matrix multiplication of two vectors given as $\bar{a} \times \bar{b} \rightarrow \sum_{y=1}^{n_y} a^y * b^y$. We further consider different types of probability in this work where $\bar{p}_i(x_i)$ is for a successful of attack depends on time t. To that end, with security investments x_i, the expected amount of breaches is a vector of $\bar{p}_i(x_i)$, and if we know how each vulnerabilities $\bar{V}_i$ in the system leads to a single loss expectancy for every single threat occurrence $\bar{L}_i = \langle L^1, L^2, ..., L^{n_y} \rangle$, we are able to compute the overall loss in T period, i.e. risk:

$$risk(x_i) = \bar{p}_i(x_i) \times \bar{L}_i \tag{1}$$

So far, an organization i possesses the following wealth after T period considering two cases; either with or without loss:

$$\begin{aligned} W_i^L &= W_i^0 - x_i - \bar{L}_i \qquad with \quad Loss \quad (\bar{p}_i(x_i) > 0) \\ W_i^N &= W_i^0 - x_i \qquad without \quad Loss \quad (1 - \bar{p}_i(x_i)) \end{aligned} \tag{2}$$

Since, in this work, an organisation i is allowed to purchase insurance, it pays a premium π_i in order to cover its losses in case of an incident with indemnity[4] that is denoted by $\bar{I}_i$, $\bar{I}_i \leq \bar{L}_i$). The premium is assumed to be equal with the risk of an insured we aforementioned, $\pi_i = \bar{p}_i(x_i) \times \bar{L}_i$, if the insurance

[4]a fee from insurer to insured

market is considered a competitive, i.e. no insurer can propose a better contract than others [3].

Current literature, i.e. [8], [15], [40], mostly consider that the probability of attack is given to the model and do not compute it with assuming practical scenarios. We let K be a set of available countermeasures that an organization is able to install and $K_i \subset K$ be the set of countermeasures that the organization decides to install. If there is neither security investments nor countermeasures, $x_i = 0$ and $K_i = \emptyset$, the likelihood of attack (as called frequency of threat occurrence in some cases) is equal to initial security investments and it can be found based on some statistic data or we may assume it since the last security investments. At the initial pace, we speculate that the selected countermeasures are efficient enough to decrease the $\bar{V}_i$ and $\bar{p}_i(x)$ and increase t, and we re-write the probability of attack an organization as $\bar{p}_i(x_i|K_i)$ with the consideration that this computation comprises the likelihood of attack when there is no investments at all.

Finally, similar to other economic models [3], [8], [9], we reason with the utility of possessing certain amount of wealth ($U_i(W_i)$), rather than with the wealth itself W_i. The utility function is considered to be continuous non-decreasing concave, i.e. $U'(W) > 0$ and $U''(W) < 0$. Let $\bar{z}_i = \langle z^1, z^2, ..., z^{n_y} \rangle$ be a random vector of numbers of threat occurrences (one per threat) and $p_i(\bar{z}|K_i, x_i)$ be the probability that the organization i will face $\bar{z}$ incidents in the T period of time under the condition that investments in self-protection are x_i and implemented countermeasures are K_i. Also, $\bar{p}_i(K_i|x_i) = \sum_{\forall \bar{z}} p_i(\bar{z}|K_i, x_i) \circ \bar{z}$ where $\circ$ refers the Hadamard product of two vectors $\bar{a}$ and $\bar{b}$ that is denoted as $\bar{c} = \langle a^1 * b^1, a^2 * b^2, ..., a^{n_y} * b^{n_y} \rangle$. The expected wealth is the amount left after subtraction from the initial wealth the premium, the self-investments, and the loss:

$$W(\bar{z}, x_i, \bar{I}_i, K_i) = W^0 - (\bar{p}_i(K_i|x_i)) \times \bar{I}_i - x_i - \bar{z} \times (\bar{L}_i - \bar{I}_i), \tag{3}$$

$$U(\bar{z}, x_i, \bar{I}_i, K_i) = U(W^0 - (\bar{p}_i(K_i|x_i)) \times \bar{I}_i - x_i - \bar{z} \times (\bar{L}_i - \bar{I}_i)). \tag{4}$$

$$where\ \bar{I}_i - \bar{L}_i = \langle I^1 - L^1, I^2 - L^2, ..., I^{n_y} - L^{n_y} \rangle.$$

Finally, the expected utility is equal to:

$$E[U] = \\ = \sum_{\forall \bar{z}} p_i(\bar{z}|K_i, x_i) U(W^0 - (\bar{p}_i(K_i|x_i)) \times \bar{I}_i - x_i + \bar{z} \times (\bar{I}_i - \bar{L}_i)), \tag{5}$$

The goal of the organisation, is to maximise the expected utility ($\max_{x_i, \bar{I}_i, K_i} E[U]$) by selecting x_i, $\bar{I}_i$ and K_i.

Problem Statement 1 *Find the most efficient distribution of security expenditure for cyber insurance π_i, and security investments x_i in a competitive insurance market, by defining "t, $\bar{I}_i$, $\bar{p}_i(x_i(t))$, K_i" when the security investments model is discrete.*

IV. Proposed Solution

We propose a solution based on vulnerability and risk assessments where the outputs become an input to our approach. The following framework, Figure 1, presents the main insight into our solution after finding the optimal indemnity pace. We first define the optimal indemnity for the insured

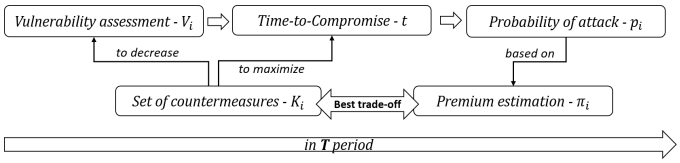

Fig. 1. Proposed solution

assuming that the insurance market type is competitive, and then look for the best security distribution for cyber insurance and countermeasures. A selection process of countermeasures allows us to decrease the loss in a way of decreasing the number of vulnerabilities $\bar{V}_i$ in the organization. In order to find the probability of attack $\bar{p}_i(x_i)$, we review and adapt some existing time-to-compromise approaches [29]–[31]. In this work, the selection process of the best set of countermeasures changes the time-to-compromise metric, i.e. K_i^* is the best set for the maximum $t \in T$. In time-to-compromise formulas, there is another type of probabilities, an attacker is able to exploit the system, which is differently specified than $\bar{p}_i(x_i)$. These probabilities help us to find the time to compromise the system t where we use that time to define the probability of attacking p_i the organization i. Once we define the probability of attack considering the time to compromise for different phases (i.e. an attacker knows both known vulnerabilities and exploits to attack a system), we are able to estimate the cyber risk, a fundamental part of cyber insurance premium estimation. To solve this, we refer the interested readers to our last work [15] based on a multi-objective knapsack problem. We proposed a solution to find the optimal security expenditure for cyber insurance and security investments. We modify and extend the idea of finding the best distribution in this work, by ensuring the maximum t based on K_i, and decreasing the $\bar{V}_i$. More importantly, we find the probability of attack $\bar{p}_i(x_i)$ in this work which was presumable given in the previous work [15].

A. Indemnity

Our first goal is to find the optimal indemnity $\bar{I}_i$ which can maximize the expected utility of an organization i, with taking into account the first order condition (FOC). First we transfer our Equation 5 and apply Jensen's inequality for a concave function (for any concave function $\phi(r)$ $E[\phi(r)] \leq \phi(E[r])$):

$$\sum_{\forall \bar{z}} p_i(\bar{z}|K_i, x_i) U(W^0 - (\bar{p}_i(K_i|x_i)) \times \bar{I}_i - x_i + \bar{z} \times (\bar{I}_i - \bar{L}_i)) \leq$$

$$U(\sum_{\forall \bar{z}} p_i(\bar{z}|K_i, x_i) \left[W^0 - (\bar{p}_i(K_i|x_i)) \times \bar{I}_i - x_i + \bar{z} \times (\bar{I}_i - \bar{L}_i)\right]) =$$

$$U(\left[\sum_{\forall \bar{z}} p_i(\bar{z}|K_i, x_i)\right](W^0 - x_i) - \left[\sum_{\forall \bar{z}} p_i(\bar{z}|K_i, x_i)\right][(\bar{p}_i(K_i|x_i)) \times$$

$$\times \bar{I}_i] + \left[\sum_{\forall \bar{z}} p_i(\bar{z}|K_i, x_i) \circ \bar{z}\right] \times \bar{I}_i - \left[\sum_{\forall \bar{z}} p_i(\bar{z}|K_i, x_i) \circ \bar{z}\right] \times \bar{L}_i).$$

Since $\sum_{\forall \bar{z}} p_i(\bar{z}|K_i, x_i) = 1$ and $\bar{p_i}(K_i|x_i) = \sum_{\forall \bar{z}} p_i(\bar{z}|K_i, x_i) \circ \bar{z}$, we get:

$$U(W^0 - x_i - \left[(\bar{p_i}(K_i|x_i)) \times \bar{I_i}\right] + (\bar{p_i}(K_i|x_i)) \times \bar{I_i} - (\bar{p_i}(K_i|x_i)) \times \\ \times \bar{L_i}) = U(W^0 - x_i - (\bar{p_i}(K_i|x_i)) \times \bar{L_i}).$$

The last part $(U(W^0 - x_i - (\bar{p_i}(K_i|x_i)) \times \bar{L_i}))$ is the expected utility if $\bar{I_i} = \bar{L_i}$. In other words, Equation 5 is maximal if $\bar{I_i} = \bar{L_i}$.

B. Time to compromise model

As we aforementioned, the probability of attack $\bar{p_i}(x_i)$ is correlated to time t that an attacker needs to compromise the organization. Also, this correlation was either scientifically or statistically addressed in several papers [29]–[31], such as Mcqueen et al. [30] proposed a model to define time to compromise a system. It further indicates that, as time increases for the organization, the probability of being attacked by an attacker increases [29]. However, we limit this time by T, assuming that cyber insurance policy is better off for both insured and insurer in a certain time with the initial security expenditure. On the other hand, we assume that an attacker stops at a certain point where his/her benefit is less than an effort or cost he/she puts on. Finding the time to compromise a system, we are able to compute the probability of attack $\bar{p_i}(x_i)$.

In order to define or predict the time to compromise a system t, we adapt a model by Mcqueen [30] which was improved by a recommendation in the model of William et al. [34]. The authors addressed different phases as follows:

1) Phase 1 - where a system has at least one vulnerability is known as well as exploit is available, where the probability of an attacker comprises a system is denoted as $P_{v,exp}$.
2) Phase 2 - where a system has at least one vulnerability to exploit, but no known exploit is available, and the probability for this phases is $P_{v,noexp}$.
3) Phase 3 - is the identification of unknown vulnerability and exploit, $P_{nov,noexp}$.

We denote V_i as the number of vulnerabilities and M_i as the number of known exploits. Also, NVD is the non-duplicate vulnerability in National Vulnerability Database.

$$t = \tau_1 \cdot P_{v,exp} + (1 - P_{v,exp})(\tau_2 P_{v,noexp} + \\ + \tau_3 \cdot (1 - P_{v,noexp}) P_{nov,noexp}) \qquad where \\ P_{v,exp} = Pr\left[\exists known(v) \wedge has(i,v) \wedge exploit(v)\right] = \\ = 1 - e^{-|V_i||M_i|/|NVD|}, \\ P_{v,noexp} = Pr\left[\exists known(v) \wedge has(i,v) \wedge \neg exploit(v)\right] = \\ = 1 - e^{-|V_i|/|NVD|}, \\ P_{v,noexp} = Pr\left[\forall known(v) \neg has(i,v) \wedge \neg exploit(v)\right] = \\ = (1-s)^{|V_i|} \cdot e^{-|V_i||M_i|/|NVD|}. \tag{6}$$

, τ_1, τ_2, τ_3 reveals the required time for each phase and s presents that a level of an attacker, comprising novice, beginner, intermediate and expert. The probability of finding a zero-day vulnerability and creating an exploit considerably depends on the level of the attacker's skill s. As thereof Equation 6, we adapted the model [30] and presented in a plain way in terms of the probability of attack for each phase. For instance, $Pr\left[\exists known(v) \wedge has(i,v) \wedge exploit(v)\right]$ presents the probability if there is a known vulnerability $v \in V_i$ in the organization i and there is at least one available exploit for this vulnerability. Now if we can find the each required time $\tau_1,\ \tau_2,\ \tau_3$, we are able to define the overall time to compromise the system which leads us to compute the $\bar{p_i}(x_i)$.

a) time 1: We took into account an experimental work conducted by Jonsson et al. [41] which reveals that two novice attackers can compromise the system with a given vulnerability in 4 hours. Thus, each attacker can take around 8 hours, a working day, as the mean time for a successful attack. However, exploiting a vulnerability depends on the severity level of vulnerability score which was proposed in [34]. In this regard, our t_1 is given:

$$\tau_1 = 1\ day * \frac{10}{cvss(e)} \tag{7}$$

where cvss(e) represents the mean CVSS score of the vulnerabilities V_i being exploited. It may lead us to a range from 1 day to about 6 days due to the current smallest CVSS score around 1.7 [42]. Yet, it becomes more accurate based on specific applications' needs.

b) time 2: The mean time τ_2 for the phase two depends on the known vulnerability and the overall vulnerabilities in NVD. Also, we simply assume that if an attacker is either novice or beginner, there is no chance of creating an exploit to available vulnerabilities. For those who are capable of creating an exploit, the chance of compromising a system depends on the mean CVSS score. In this phase, without a known exploit for the vulnerability, we have derived the average time for the new exploit code announcement. Thus, this time, 5.8 days in average, is the baseline of phase 2 time estimation. Now, the overall time is calculated as follows:

$$\tau_2 = 5.8\ days * \frac{10}{cvss(e)} \tag{8}$$

c) time 3: The mean time for the next vulnerability announcement is constant and could not be changed over time according to Rescorla's research [43]. Even though it is an ideal case, we would like to adapt this number, 30.42 days, for the time between new vulnerabilities. Since both vulnerabilities and exploits are unknown, there is a need for a combination of the time for the announcement of known vulnerabilities and exploits. But also the s is the appropriate value based on the attacker's skill level. We consider an attacker in different groups which were classified by their level of skills. N.Paulauskas et al. [31] proposed that beginner skill level interval to be between 0.1 to 0.6, intermediate between 0.6 to 0.8, and expert 0.8 to 1. Furthermore, there is another classification that adds a novice attacker into the list whose level of skill is up to 0.15.

$$\tau_3 = ((1/s - 0.5) \cdot 30.42 + 5.8 days) * \frac{10}{cvss(e)}\ days \tag{9}$$

Finally, we are able to compute our time-to-compromise t as the following way:

$$t = \tau_1(1 - e^{-|V_i||M_i|/|NVD|}) + \tau_2 e^{-|V_i||M_i|/|NVD|}(1 - e^{-|V_i|/|NVD|}) + \tau_3(1 - s)^{|V_i|} e^{-|V_i|(2|M_i|+1)/|NVD|} \quad (10)$$

,where τ_1, τ_2, τ_3 will be replaced with the aforementioned Equations. Now our solution depends on the number of vulnerabilities in a system that can be decreased by the selection of countermeasures K_i.

C. Security controls

Since our analysis shows $\bar{I}_i = \bar{L}_i$, our maximisation problem (Equation 5) turns into the following equation:

$$\max_{x_i, K_i} U(W^0 - x)i - (\bar{p}_i(K_i|x_i)) \times \bar{L}_i). \quad (11)$$

We presumably consider that the initial wealth W^0 is fixed and utility function is non-decreasing. To that end, instead of maximizing the utility function, we simply minimize the sum of security investments x_i and premium π_i which is equal to $(\bar{p}_i(K_i|x_i)) \times \bar{L}_i$.

$$\min_{x_i, K_i}(x_i + (\bar{p}_i(K_i|x_i)) \times \bar{L}_i). \quad (12)$$

To minimize this sum we need to select the best set of countermeasures K_i which is required to be less or equal to the security investments x_i. Since the utility function $U()$ is concave and the K_i affects the π_i estimation, K_i is the key component to minimize the sum.

We let $\gamma_k \in [0, 1]$ be the capability of countermeasure to remove the number of vulnerabilities $\bar{V}_i$ of an organization i. For instance, if $\gamma_k = 0.3$, the countermeasure removes the 30% of all vulnerabilities $\bar{V}_i$. However, the selection process of countermeasures inevitably considers the loss that a vulnerability leads to. Considering that we have a set of installed countermeasures which are correlated each other, we are able to compute the overall capability of countermeasures as is given:

$$\bar{\gamma}(K_i) = \prod_{\forall k \in K_i} \bar{\gamma}(k), \quad (13)$$

where $\prod_{\forall k \in K_i}$ stands for the Hadamard product.

Moreover, choosing an appropriate and efficient countermeasure depends on its cost, denoted as function c and is assumed to provide a finite non-negative integer value $c : K \mapsto \mathbb{N}^+$. The overall cost of installed countermeasures $K_i \subseteq K$ $(c(K_i))$ can be computed as:

$$c(K_i) = \sum_{\forall k \in K_i} c(k). \quad (14)$$

Now, we are able to connect $\bar{\gamma}(K_i|x_i)$ and $\bar{p}_i(x_i)$. The most efficient money distribution (minimal expenditure) is if K_i minimises the premium:

$$\min_{\forall K_i \subset K}(\left[\prod_{\forall k \in K_i}(1 - \bar{\gamma}(k))\right]) \times \bar{L}_i \quad and \quad \sum_{\forall k \in K_i} c(k) \leq x. \quad (15)$$

The sub-problem of finding the optimal set of countermeasures K_i^*, for which we say that $\bar{p}_i(K_i^*|x_i) = \bar{p}_i(x_i))$ reminds 0-1 multi-objective knapsack problem [44], but instead of summing of values per objectives, we multiply them, and thus, look for the minimal overall value (capability of decreasing the most number of vulnerabilities $\bar{V}_i$). It is worthwhile that our capability of a countermeasure γ_k will be turned into $1 - \gamma_k$ in our algorithmic solution, since we are aiming at the minimization of the probability.

D. Algorithm

So far, we have found the optimal indemnity which is equal to the loss and defined a method to compute the time to compromise. Moreover, we connect the vulnerabilities of a system to the probability of attack by defining the potential countermeasures that decrease the number of vulnerabilities. Yet, we have not described our solution to find the best set of countermeasures which satisfies the maximum utility of an insured. In this part, we introduce a way of finding the best distribution of security expenditure between cyber insurance and security investments based on our last work [15] where we adapted and modified a multi-objective knapsack problem. The dynamic programming was the proposed solution and it looks for the minimal probability of survival that a threat passes which is equal to $1 - \gamma_k$ in this work. Our algorithm solves the problem in different way than a general knapsack problem does, by incrementing the security investments from zero until it finds the optimal investments. We refer interested readers to [15] for perceiving a better explanation of what we proposed and how the whole solution and algorithm work. We keep our main algorithm (see in [15]) in this work by replacing some values, i.e. $\bar{\gamma}$ has been introduced. We further present an extension of the algorithm (Algorithm 1), where both probability of attack $\bar{p}_i(x_i)$ and time to compromise t are computed based on vulnerabilities $\bar{V}_i$. Our main contribution is that we ensure one more condition, selecting the best set of countermeasures to satisfy the longest t and finds the optimal investments x_i^*, in comparison with our last work. In algorithm 1, we start with the values that we defined above and find the number of vulnerabilities in line 12. We simply postulate the cvss score as a mean score of remained vulnerabilities in line 13. Finally, time to compromise metric is calculated in line 14, where we suppose that M_i is a number of available exploits for the vulnerabilities after installing countermeasures.

E. Probability of attack

So far, we have computed the time to compromise t_i based on both selection of countermeasures K_i and probabilities that an attacker q is able to find or exploit the vulnerabilities V_i as is referred in *Equation* 6. Now, our goal is to find the overall probability of attack $p_i(x_i)$ if K_i countermeasures are installed.

So far, we did not put any limitation on how much resources, i.e., time in our paper, an attacker is ready to devote to compromise the system. In reality, an attacker will simply switch to another target if the system he is trying to attack is too strong. Let t' denote the time that an attacker is ready

Algorithm 1 Compute the time to compromise t

procedure COMPUTETIMETOCOMPROMISE(K_i, V_i, $\gamma(K_i)$, M_i, NVD, τ, s, $cvss(e)$, t)
Require: τ ▷ - time to exploit a vulnerability in system for each phase
Require: t ▷ - time to compromise
$cvss(e)$: ▷ - mean score for the vulnerabilities in a system
s: ▷ - attacker's level of skill
$\bar{\gamma} : K_i \mapsto 2^{[0;1]}$ ▷ - capability function of a countermeasure to decrease the number of vulnerabilities
$\bar{V}_i \in \mathbb{N}$ ▷ - a number of vulnerabilities in a system
$M_i \in \mathbb{N}$ ▷ - a number of known exploits for existing vulnerabilities V_i
$NVD \in \mathbb{N}$ ▷ - non-duplicated number of vulnerabilities in National Database

$\tau_1 = 1\ day * \frac{10}{cvss(e)}$
$\tau_2 = 5.8\ days * \frac{10}{cvss(e)}$
$\tau_3 = ((1/s - 0.5) \cdot 30.42 + 5.8 days) * \frac{10}{cvss(e)}\ days$
$V_i \leftarrow V_i * (1 - \gamma(K_i))$ ▷ vulnerabilities of a system after installed countermeasures
$cvss(e) \leftarrow cvss(e)_{V_i}$ ▷ mean CVSS score to exploit remained vulnerabilities V_i after installing countermeasures K_i
$t = \tau_1(1 - e^{-|V_i||M_i|/|NVD|}) + \tau_2 e^{-|V_i||M_i|/|NVD|}(1 - e^{-|V_i|/|NVD|}) + \tau_3(1 - s)^{|V_i|} e^{-|V_i|(2|M_i|+1)/|NVD|}$ ▷ Compute the time to compromise based on our best countermeasures
return $[t]$
end procedure

to devote and stops attempting to compromise the system after this time. In other words, if the expected benefits become smaller than the cost of compromising the system, an attacker stops attempting.

In the simplest case, if $t \leq t'$ the attacker will compromise the system and it will fail otherwise. We may also assume some distribution of attackers with respect to the time they are ready to devote for compromising the system ($Pr[\tau < t']$, if τ is a random variable). If we use t as a limit, we will be able to find the probability that the attacker is able to compromise the system: $p_i(t(x_i)) = Pr[\tau < t]$. Although, $Pr[\tau < t']$ is not trivial to find, we would like to note that this parameter does not depend on the internal structure (the security protection) of the system, i.e., can be evaluated by external experts and used by the organisation.

V. Discussion and Future work

Our initial step of applying time to compromise approach to cyber insurance is opening the promising ways to deal with the challenges. We expect that the idea allows cyber insurance to become more dynamic like other insurance cases, i.e. travel insurance [45]. In this section, we present what has been introduced in this paper and what will be the next steps we are aiming at.

a) Vulnerability assessment is a vital part.: The vulnerability assessment (hereinafter VA) is the fundamental part of our solution, which provides the number of available vulnerabilities and known exploits to them. In the current situation, for organizations, a well-known method to deal with cyber risks is to follow the security standards (NIST, ISO/SEC 27001 e.g.) in order to mitigate the risks with having different security controls. Yet, the dependency of security controls and vulnerabilities are not thoroughly studied and there is no approach to connect this dependency with cyber insurance model. Since the information of vulnerabilities can be obtained by conducting VA for almost all organizations, we strongly believe that looking forward to extending this idea is a promising idea. In particular, VA is one of the applicable ways to compute the probability of attack quantitatively, i.e. [32].

b) Countermeasures.: We have defined the interplay of countermeasures and cyber insurance based on a multiple-objective knapsack problem which looks for the best set of security countermeasures by decreasing the number of vulnerabilities. So far, we considered the dependency of countermeasures, vulnerabilities and cyber insurance without either any security interdependency[5]. We will further consider the impact of security interdependency on optimal selection.

c) Time to compromise.: The main instrument of this paper is applying time to compromise model to cyber insurance and enunciating the dependency of the probability of attack and required time to compromise. An approach we applied in this work considers some fixed numbers for defining the time for an attacker either to exploit the vulnerability or create one, which some may argue that these numbers are unreasonable or should be updated. However, we adapted this model due to its connectedness with vulnerabilities which can be obtained and believed that these times (τ_1, τ_2, τ_3) can be updated by conducting with some experimental works or with empirical data. More importantly, we expect that finding t and improving the modus operandi of computing t is a key to both find the $p_i(t(x_i))$ and re-define T. In other words, we would like to devise an approach to offer different durations for cyber insurance policy based on insured's level of security and wish of underwriting the policy with different durations, through changing T.

VI. Conclusion

We introduced an approach to find the optimal distribution of security expenditure for cyber risk mitigation and transfer techniques based on a multi-objective knapsack problem. This work presents a solution to compute the probability of attack based on vulnerabilities of a system which is available to any organization. We selected the best set of countermeasures which decreases the vulnerabilities of a system at most and introduced the dependency of vulnerabilities, security investments and cyber insurance model. In particular, we applied

[5]a degree which expresses how one's level of security is affected by its neighbour's security investments

time to compromise metric to cyber insurance model, which helps both insurers and insureds to capture the challenges. We found that a chance of an organization is being attacked by an attacker increases from time t to t'.

We further validate our work based on experimental work comparing different systems and improve our model. Moreover, our goal is to make a cyber insurance policy more dynamic by offering different cyber insurance policies with various durations. Last but not least, we would like to investigate the impact of cyber security interdependence on a decision making of countermeasure selection and time to compromise computation.

REFERENCES

[1] Available via https://www.nbcnews.com/tech/internet/after-huge-global-cyberattack-countries-scramble-halt-spread-ransomware-n759121

[2] Symantec: Internet Security Report. Volume 23, 2018. available via https://www.symantec.com/security-center/threat-report

[3] A.Marotta, F.Martinelli, S.Nanni, A.Orlando, A.Yautsiukhin: Cyber-insurance survey. Computer Science Review 24, 35–61 (May 2017)

[4] Cisco: Annual Cybersecurity Report, available via http://www.cisco.com/go/acr2017, 2017.

[5] Anderson, Ross, and Tyler Moore. "The economics of information security." Science 314, no. 5799 (2006): 610-613.

[6] PwC: Global Cyber Insurance Survey. available via https://www.pwc.com/us/en/industries/insurance/library/cyber-insurance-survey.html, 2018

[7] R.Anderson, R.Böhme, R.Claytin, T.Moore: Security economics and the internal market, January 2008.

[8] H.Ogut, N.Menon, S.Raghunathan: Cyber insurance and it security investment: Impact of interdependent risk. In: Proceedings of the 4th Workshop on the Economics of Information Security, 2005.

[9] I.Ehrlich, G.S.Becker: Market Insurance, Self-Insurance, and Self-Protection Foundations of Insurance Economics:, chap. Economics and Finance, pp. 164–189. Springer Netherlands, 1992.

[10] G.A.Schwartz, S.S.Sastry: Cyber-insurance framework for large scale interdependent networks. In: Proceedings of the 3rd International Conference on High Confidence Networked Systems, HiCoNS '14,. pp. 145–154. ACM, 2014.

[11] G.A. Schwartz, S.S. Sastry, Cyber-insurance framework for large scale interdependent networks, in: Proceedings of the 3rd International Conference on High Confidence Networked Systems, HiCoNS'14, ACM, New York, NY, USA, 2014, pp. 14-154.

[12] N.Shetty, G.Schwartz, J.Walrand: Can competitive insurers improve network security? In: A.Acquisti, S.Smith, A.R.Sadeghi (eds.) Proceedings of the 3rd International Conference on Trust and Trustworthy Computing,, Lecture Notes in Computer Science, vol. 6101, pp. 308–322. Springer (2010)

[13] Z. Yang, J.C.S. Lui, Security adoption and influence of cyber-insurance markets in heterogeneous networks, Perform. Eval. 74 (2014) 1-17.

[14] M.Lelarge, J.Bolot: Economic incentives to increase security in the internet: The case for insurance. In: Proceedings of the 28th IEEE International Conference on Computer Communications,. pp. 1494–1502, April 2009.

[15] Martinelli, Fabio, Ganbayar Uuganbayar, and Artsiom Yautsiukhin. "Optimal Security Configuration for Cyber Insurance." In IFIP International Conference on ICT Systems Security and Privacy Protection, pp. 187-200. Springer, Cham, 2018.

[16] PartnerRe: Survey of Cyber Insurance Market Trends. available via https://partnerre.com/, 2017.

[17] Bolot, Jean, and Marc Lelarge. "Cyber insurance as an incentivefor Internet security." In Managing information risk and the economics of security, pp. 269-290. Springer, Boston, MA, 2009.

[18] Kesan Jay, Ruperto Majuca, and William Yurcik. "Cyberinsurance as a market-based solution to the problem of cybersecurity: a case study." In Proc. WEIS, pp. 1-46. 2005.

[19] Khalili, Mohammad Mahdi, Parinaz Naghizadeh, and Mingyan Liu. "Designing cyber insurance policies in the presence of security interdependence." In Proceedings of the 12th workshop on the Economics of Networks, Systems and Computation, p. 7. ACM, 2017.

[20] ENISA: Incentives and barriers of the cyber insurance market in europe, available via http://www.goo.gl/BtNyj4 on 12/12/2014, June 2012.

[21] R.Pal, L.Golubchik, K.Psounis, P.Hui: Will cyber-insurance improve network security? a market analysis. In: Proceedings of the 2014 IEEE Conference on Computer Communications. pp. 235–243. IEEE (2014)

[22] Schneier, Bruce. "Insurance and the computer industry." Communications of the ACM 44, no. 3 (2001): 114-114.

[23] R.P.Majuca, W.Yurcik, J.P.Kesan.: The evolution of cyberinsurance. The Computing Research Repository pp. 1–16, 2006.

[24] Martinelli, Fabio, Albina Orlando, Ganbayar Uuganbayar, and Artsiom Yautsiukhin. "Preventing the drop in security investments for non-competitive cyber-insurance market.". In: Proceedings of the 12th International Conference on Risks and Security of Internet and Systems, (will be appeared in Springer). 2017.

[25] N. Shetty, G. Schwartz, M. Felegyhazi, J. Walrand, Competitive cyberinsurance and internet security, in: Economics of Information Security and Privacy, Springer, US, 2010, pp. 229-247.

[26] S. Gritzalis, A.N. Yannacopoulos, C. Lambrinoudakis, P. Hatzopoulos, S.K. Katsikas, A probabilistic model for optimal insurance contracts against security risks and privacy violation in it outsourcing environments, Int. J. Inf. Secur. 6 (4) (2007) 197-211.

[27] R.S. Betterley, Cyber/privacy insurance market survey - 2014, available via http://betterley.com/samples/cpims14_nt.pdf on 03/01/2017 (June 2014).

[28] Bandyopadhyay, Tridib. "Organizational adoption of cyber insurance instruments in IT security risk management: a modeling approach." Proceedings. Paper 5 (2012).

[29] Littlewood, Bev, Sarah Brocklehurst, Norman Fenton, Peter Mellor, Stella Page, David Wright, John Dobson, John McDermid, and Dieter Gollmann. "Towards operational measures of computer security." Journal of computer security 2, no. 2-3 (1993): 211-229.

[30] McQueen, Miles A., Wayne F. Boyer, Mark A. Flynn, and George A. Beitel. "Time-to-compromise model for cyber risk reduction estimation." In Quality of Protection, pp. 49-64. Springer, Boston, MA, 2006.

[31] Paulauskas, N., and E. Garsva. "Attacker skill level distribution estimation in the system mean time-to-compromise." In Information Technology, 2008. IT 2008. 1st International Conference on, pp. 1-4. IEEE, 2008.

[32] Allodi, Luca, and Fabio Massacci. "Security Events and Vulnerability Data for Cybersecurity Risk Estimation." Risk Analysis 37, no. 8 (2017): 1606-1627.

[33] Leversage, David John, and Eric James Byres. "Estimating a System." IEEE Security & Privacy 1 (2008): 52-60.

[34] Nzoukou, William, Lingyu Wang, Sushil Jajodia, and Anoop Singhal. "A unified framework for measuring a network's mean time-to-compromise." In Reliable Distributed Systems (SRDS), 2013 IEEE 32nd International Symposium on, pp. 215-224. IEEE, 2013.

[35] Smeraldi, Fabrizio, and Pasquale Malacaria. "How to spend it: optimal investment for cyber security." Proceedings of the 1st International Workshop on Agents and CyberSecurity. ACM, 2014.

[36] Sawik, Tadeusz. "Selection of optimal countermeasure portfolio in IT security planning." Decision Support Systems 55.1 (2013): 156-164.

[37] Fielder, Andrew, et al. "Decision support approaches for cyber security investment." Decision Support Systems 86 (2016): 13-23.

[38] Bartholdi III, John J. "The knapsack problem." Building Intuition. Springer US, 2008. 19-31.

[39] Leanid Krautsevich and Aliaksandr Lazouski and Fabio Martinelli and Artsiom Yautsiukhin. "Risk-Based Usage Control for Service Oriented Architecture." In Proceedings of the 18th Euromicro International Conference on Parallel, Distributed and Network-Based Computing, 2010.

[40] Böhme, Rainer, Stefan Laube, and Markus Riek. "A Fundamental Approach to Cyber Risk Analysis." Variance Journal, Article (2017).

[41] Jonsson, Erland, and Tomas Olovsson. "A quantitative model of the security intrusion process based on attacker behavior." IEEE Transactions on Software Engineering 23, no. 4 (1997): 235-245.

[42] OF STANDARDS, N. I., AND TECHNOLOGY. National vulnerability database version 2.2. http://nvd.nist.gov/.

[43] E. Rescorla, "Is Finding Security Holes a Good Idea?" IEEE Security & Privacy, vol. 3, no. 1, Jan./Feb. 2005, pp. 14âĂŞ19.

[44] Bazgan, Cristina, Hadrien Hugot, and Daniel Vanderpooten. "Solving efficiently the 0 – 1 multi-objective knapsack problem." Computers & Operations Research 36, no. 1 (2009): 260-279.

[45] Travel insurance through Europe Assistance. Available via https://www.europ-assistance.com/