Optimal Security Configuration for Cyber Insurance

Fabio Martinelli, Ganbayar Uuganbayar, Artsiom Yautsiukhin

Optimal security configuration for cyber insurance*

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

[1] Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, Pisa, Italy,
[2] Department of Information Engineering and Computer Science (DISI), University of Trento, Italy,
{ganbayar.uuganbayar, artsiom.yautsiukhin, fabio.martinelli}@iit.cnr.it[1]
ganbayar.uuganbayar@unitn.it[2]

Abstract. Losses due to cyber security incidents could be very significant for organisations. This fact forces managers to consider cyber security risks at the highest management level. Cyber risks are usually either mitigated by technical means (countermeasures) or transferred to another party (i.e., insurer). Both options require significant investments and organisations face the problem of optimal distribution of cyber security budget between these risk treatment options.
In this paper, we propose an approach for optimal distribution of investments between self-protection and cyber insurance. The key difference of our paper with respect to others in the field is that our model helps to identify the required security controls, rather than implicitly assuming a relation between security investments, security configuration and expected probability of attack. Our approach exploits a discrete model of investment in self-protection, which is more challenging for analysis but is more realistic and convenient for the application. Our model further considers several threats and allows threats to occur more than once.

Keywords: security investment, optimal investment, knapsack problem, cyber insurance, risk management

1 Introduction

One of the biggest challenges organisations face is the protection of their valuable assets against cyber attacks. Symantec report [1] reveals that more than 7.1 billion identities had been exposed due to data breaches within the last eight years. Although most organisations believe in their security, around 30% of them are breached in reality (according to the annual Cisco report (2017)[2]). Thus, there is always a residual risk which cannot be eliminated with technical means.

The residual risk could be either accepted or insured, i.e., transferred to another party (so-called insurer) in return for a premium, a fee an organisation

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

(called insured) pays to an insurer in return for risk coverage. Since cyber insurance was introduced, the market has been growing [4, 3, 5], although slower than predicted because of a number of challenges this young market faces.

Availability of cyber insurance market makes organisations to decide whether to buy cyber insurance or invest in self-protection. Some researchers adapted models from general insurance for analysis of various properties of cyber insurance market and security levels of organisations and society, in general. In particular, many authors tried to answer whether cyber insurance is an incentive for security investments or it is not [6, 13, 15, 11, 10]. However, some of these authors [13, 15, 11] consider a continuous investment model (any investment in self-protection reduces the probability of an incident). On the other hand, an organisation invests in self-protection by implementing various countermeasures, i.e., discretely. Other researchers, i.e., [6, 12], use an oversimplified discrete model of security investment, which simply assigns low or high level of security depending on whether investments exceed some threshold. Such model is not realistic either, as it does not allow improving security (i.e., reducing the probability of attack) if the threshold is not crossed. Moreover, both these models do not explain how the probability of attack could be computed and do not provide a way to establish the link with the available countermeasures for installation. Thus, these models cannot help to decide how to improve their cyber security.

In this paper, we provide an approach for optimal distribution of investments between cyber insurance and self-protection. The key difference of our approach with others is the discrete model of cyber security investments, explicitly taking into account the contribution of the security controls which are or can be implemented. Such an approach will help organisations to make the decisions on which countermeasures to install, keeping in mind that the rest of residual risk will be covered by cyber insurance. We consider a competitive cyber insurance market where insurers are non-profitable and assume a generic utility function without either information asymmetry or security interdependence.

The remainder of the paper unfolds as follows. In *Section* 2, we provide the basic formalisation to clarify the problem statement. We further analyse the problem and propose our solution in *Section* 3. *Section* 4 contains an example of application of our solution. We follow with a literature review (5) and then draw our conclusion (6).

2 Problem Specification

Consider an organisation which would like to devise the most efficient strategy for security investments, combining risk mitigation and risk transfer. Risk mitigation requires specification of additional security controls for self-protection and cyber insurance needs the decision on the amount of insurance coverage (indemnity) to be bought. The goal of this paper is to combine these options efficiently.

Let W be some amount of wealth an agent expects to possess after some period of time, assuming that initial wealth is W^0. Let TR be a set of size n_t ($n_t \in \mathbb{N}^+$) of all possible threats. Let $pr^q(x) \in [0; 1]$ be the probability of

W^0 - initial wealth	$\bar{\pi}$ - probability of a threat *survival*
x - security investment	$\bar{F}$ - expected number of threat *attempts*
c - cost of a countermeasure	$\bar{pr}$ - probability of a threat *occurrence*
P - premium	$\bar{z}$ - real *number* of threat occurrence
K - a set of *available* countermeasures	$\bar{L}$ - loss
K_i - a set of *installed* countermeasures	$\bar{I}$ - indemnity

Table 1. Notations adopted in this work

a threat $tr_q \in TR$ occurrence if the organisation invests x in self-protection. Naturally, we expect this probability to decrease with increase of investments ($\forall x_1 < x_2\ (pr^q(x_1) \geq pr^q(x_2))$. Let $\bar{pr}(x) = \langle pr^1(x), pr^2(x), ..., pr^{n_t}(x)\rangle$ be a vector of such probabilities for all threats. In the future, we always use a bar for vectors. All vectors in our paper are of size n_t. We also use superscripts for denoting a member of a vector, e.g., $pr^q(x)$, and subscripts for a more precise specification of a variable. We also use two vector operations in the paper. Hadamard product of two vectors $\bar{a}$ and $\bar{b}$, denoted as $\bar{a} \cdot \bar{b}$, is a vector $\bar{c} = \langle a^1 * b^1, a^2 * b^2, ..., a^{n_t} * b^{n_t}\rangle$. We also use the same symbol $\cdot$ for a multiplication of a vector by a scalar. Usual matrix multiplication of two vectors $\bar{a}$ and $\bar{b}$ is denoted as $\bar{a} \times \bar{b}$ and is a scalar value equal to $\sum_{q=1}^{n_t} a^q * b^q$.

Let $\bar{F} = \langle F^1, F^1, ..., F^{n_t}\rangle$ be a vector of an expected amount of breaches for some period if no countermeasures are installed. Then, with investment x, the expected amount of breaches is a vector: $\bar{F} \cdot \bar{pr}(x)$; and, if we know a single loss expectancy for every single threat occurrence $\bar{L} = \langle L^1, L^1, ..., L^{n_t}\rangle$, we are able to compute the overall expected loss for the considered period, i.e., risk:

$$risk(x) = (\bar{F} \cdot \bar{pr}(x)) \times \bar{L}. \tag{1}$$

Since the organisation is allowed to buy insurance, it pays a premium P in order to cover some part of its losses in case of an incident (called indemnity $\bar{I}$, $\forall q,\ I^q \leq L^q$). In this paper, we use a simple cyber insurance market model [13, 6, 16], called competitive market, which demands the premium to be equal to the expected losses of the insurer (as the market has so many insurers that no one is able to propose a better contract): $P(x) = (\bar{F} \cdot \bar{pr}(x)) \times \bar{I}$.

In the current literature on cyber insurance, e.g., [13], $pr^q(x)$ is simply assumed to exist and does not define how the required security level could be reached. In practice, organisations spend their money in portions buying new controls or implementing security practices. Let K be a set of available countermeasures and $K_i \subseteq K$ be a subset of these countermeasures which the organisation decides to apply. K_i is to be determined by the available amount of self-investments x (See Section 3.2), and we re-write $pr^q(x)$ as $pr^q(K_i|x)$ to explicitly indicate the dependency of the probability of survival on K_i.

Finally, similar to other economic models [23, 16, 4, 13], we reason with the utility of possessing certain amount of wealth $U(W)$, rather than with the wealth W itself. The utility function is assumed to be continuous, non-decreasing,

concave, and twice differential (i.e., $U'(W) > 0$ and $U''(W) < 0$). Let $\bar{z} = \langle z^1, z^2, ..., z^{n_t} \rangle$ be a random vector of numbers of threat occurrences (one per threat) and $pr(\bar{z}|K_i, x)$ be the probability that the company will face $\bar{z}$ incidents in the considered period of time under the condition that investments in self-protection are x and implemented countermeasures are K_i. Also, $\bar{F} \cdot \bar{pr}(K_i|x) = \sum_{\forall \bar{z}} pr(\bar{z}|K_i, x) \cdot \bar{z}$. The expected wealth is the amount left after subtraction from the initial wealth the premium, the self-investment, and the loss:

$$W(\bar{z}, x, \bar{I}, K_i) = W^0 - (\bar{F} \cdot \bar{pr}(K_i|x)) \times \bar{I} - x - \bar{z} \times (\bar{L} - \bar{I}), \tag{2}$$

$$U(\bar{z}, x, \bar{I}, K_i) = U(W^0 - (\bar{F} \cdot \bar{pr}(K_i|x)) \times \bar{I} - x + \bar{z} \times (\bar{L} - \bar{I})). \tag{3}$$

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

Finally, the expected utility is equal to:

$$E[U] = \sum_{\forall \bar{z}} pr(\bar{z}|K_i, x) U(W^0 - (\bar{F} \cdot \bar{pr}(K_i|x)) \times \bar{I} - x + \bar{z} \times (\bar{I} - \bar{L})), \tag{4}$$

The goal of the organisation, is to maximise $E[U]$ by selecting x, $\bar{I}$ and K_i.

$$\max_{x, \bar{I}, K_i} \sum_{\forall \bar{z}} pr(\bar{z}|K_i, x) U(W^0 - (\bar{F} \cdot \bar{pr}(K_i|x)) \times \bar{I} - x + \bar{z} \times (\bar{I} - \bar{L})). \tag{5}$$

3 Utility maximisation

3.1 Indemnity

Consider Equation 4 and apply Jensen's inequality for a concave function (for any concave function $\phi(t)$ $E[\phi(t)] \leq \phi(E[t])$):

$$\sum_{\forall \bar{z}} pr(\bar{z}|K_i, x) U(W^0 - (\bar{F} \cdot \bar{pr}(K_i|x)) \times \bar{I} - x + \bar{z} \times (\bar{I} - \bar{L})) \leq$$

$$U(\sum_{\forall \bar{z}} pr(\bar{z}|K_i, x) \left[W^0 - (\bar{F} \cdot \bar{pr}(K_i|x)) \times \bar{I} - x + \bar{z} \times (\bar{I} - \bar{L})\right]) =$$

$$U(\left[\sum_{\forall \bar{z}} pr(\bar{z}|K_i, x)\right] (W^0 - x) - \left[\sum_{\forall \bar{z}} pr(\bar{z}|K_i, x)\right] \left[(\bar{F} \cdot \bar{pr}(K_i|x)) \times \bar{I}\right] +$$

$$\left[\sum_{\forall \bar{z}} pr(\bar{z}|K_i, x) \cdot \bar{z}\right] \times \bar{I} - \left[\sum_{\forall \bar{z}} pr(\bar{z}|K_i, x) \cdot \bar{z}\right] \times \bar{L}).$$

Since $\sum_{\forall \bar{z}} pr(\bar{z}|K_i, x) = 1$ and $\bar{F} \cdot \bar{pr}(K_i|x) = \sum_{\forall \bar{z}} pr(\bar{z}|K_i, x) \cdot \bar{z}$, we get:

$$U(W^0 - x - \left[(\bar{F} \cdot \bar{pr}(K_i|x)) \times \bar{I}\right] + (\bar{F} \cdot \bar{pr}(K_i|x)) \times \bar{I} - (\bar{F} \cdot \bar{pr}(K_i|x)) \times \bar{L}) =$$

$$U(W^0 - x - (\bar{F} \cdot \bar{pr}(K_i|x)) \times \bar{L}).$$

The last part $(U(W^0 - x - (\bar{F} \cdot \bar{pr}(K_i|x)) \times \bar{L}))$ is the expected utility if $\bar{I} = \bar{L}$. In other words, Equation 4 is maximal if $\bar{I} = \bar{L}$.

3.2 Security controls

As $\bar{I} = \bar{L}$, our maximisation problem (Equation 5) could be reduced to:

$$\max_{x,K_i} U(W^0 - x - (\bar{F} \cdot \bar{pr}(K_i|x)) \times \bar{L}). \tag{6}$$

Since the utility function is non-decreasing, we need to maximise its argument, or simply minimise the following part (called as *expenditure* in the sequel):

$$\min_{x,K_i}(x + (\bar{F} \cdot \bar{pr}(K_i|x)) \times \bar{L}). \tag{7}$$

Since, K_i affects only $(\bar{F} \cdot \bar{pr}(K_i|x)) \times \bar{L}$ and $U()$ is concave, in order to maximise $U()$ we need to select K_i in such a way to minimise this component and we have to ensure that we do this with investments less or equal to x.

Let $\pi^q(k) \in [0; 1]$ be the probability that a threat q passes through (survives) countermeasure $k \in K_i$; countermeasure k completely eliminates threat q if $\pi^q(k) = 0$, and is entirely powerless against the threat if $\pi^q(k) = 1$. Let $\bar{\pi}(k)$ be a vector of all probabilities of survival if countermeasure k is installed, then the overall probability of survival can be computed as[3]:

$$\bar{\pi}(K_i) = \prod_{\forall k \in K_i} \bar{\pi}(k), \tag{8}$$

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

Every countermeasure has its cost, denoted as function c and is assumed to provide a finite non-negative integer value $c : K \mapsto \mathbb{N}^+$. Naturally, the cost of installed countermeasures $K_i \subseteq K$ $(c(K_i))$ can be computed as:

$$c(K_i) = \sum_{\forall k \in K_i} c(k). \tag{9}$$

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

$$\min_{\forall K_i \subset K}(\bar{F} \cdot \left[\prod_{\forall k \in K_i} \bar{\pi}(k)\right]) \times \bar{L} \quad and \quad \sum_{\forall k \in K_i} c(k) \leq x. \tag{10}$$

The sub-problem of finding the optimal set of countermeasures K_i^*, for which we say that $\bar{\pi}(K_i^*|x) = \bar{pr}(x)$ reminds 0-1 multi-objective Knapsack problem [7], but instead of summing of values per objectives, we multiply them, and, thus, look for the minimal overall value.

3.3 Security investments

Finally, we may return to the main problem, i.e., how to find the right amount of investments in self-protection. From Equation 7 investments must be as low as

[3] We assume effects of countermeasures independent from each other.

possible, but they also must be high enough to keep the insurance premium low. Moreover, the solution for Equation 7 depends on solving the 0-1 multi-objective knapsack problem Equation 10.

We propose a solution that is based on the dynamic programming algorithm for solving 0-1 multi-objective knapsack problem [7]. We assume that the cost of countermeasures could be seen as positive integer values (or, can be seen as $\forall k \in K$ $(c(k) = C * m_k)$, where C and m_k are positive natural values, and C is the greatest common divisor for countermeasures' costs). Let all elements of K be enumerated with $j = 1, ..., n_K$ (where n_K is the size of K). For every amount of investments x we consider (accept or reject) the first j countermeasures. For those accepted K_i, we compute the overall probability of threat's survival $\bar{pr}(K_i|x)$ (see Equation 8). The overall probability of survival for every K_i is stored in a corresponding cell $T[j][x]$ of an auxiliary matrix T.

Since for our problem we cannot store only the optimal value at every intermediate step (as it is done for a simple 0-1 knapsack problem), we remember (in a matrix cell $T[j][x]$) all *non-dominant* probability vectors, i.e., vectors which potentially could lead to the optimal solution. In the most simple case, we may see selection of non-dominant vectors as those which cannot be rejected using the Pareto optimality criteria (i.e., $\forall \bar{t_1}, \bar{t_2} \in T[j][x]$ $(\exists q$ $(t_1^q > t_2^q)))$. As it was shown by Bazgan et. al, [7] other dominance relations could be applied to speed up the algorithm. Since, this is not crucial for our paper, we refer the interesting reader to the original paper of the authors for a more detailed discussion on the non-dominant relations, which can be applied to our problem.

In short, the core part of the solution for 0-1 multi-objective knapsack problem could be seen as the following recursive algorithm:

1. $T[0][x] = 1$;
2. $T[j][x] = T[j-1][x]$ if $c(k_j) > x$ (the new item is more expensive than the current cost limit);
3. $$\left.\begin{array}{c} T_{add} = \bigcup\limits_{\forall \bar{t} \in T[j-1][x-c(k_j)]} \bar{t} \cdot \bar{\pi}(k_j) \\ T[j][x] = non - dominant(T[j-1][x] \cup T_{add}) \end{array}\right\} \text{ if } c(k_j) \leq x.$$

Naturally, every last cell in a column $T[n_k][x]$ returns the overall probability of survival for x investments and *all* n_k countermeasures taken into account. It is required only to find the K_i which causes the minimal total expenditure, using the vectors from $T[n_k][x]$ as $\bar{pr}(K_i|x)$ and applying Equation 7.

To get the final solution for optimal investments x^*, i.e., $T[n_K][x^*]$, we need to know x^*. It is important to note that the core part of the recursive algorithm does not require the knowledge of maximal investments in order to count values for any intermediate x. In other words, we may start the algorithm with $x = 0$ and continue as much as we need or until we find our solution (also extending matrix T for new x to check). Now, our goal is to *find the way to minimise the amount of required iterations and ensure that the solution to Equation 7 will be found.*

Let $P^*(x)$ be the optimal insurance premium if x amount of money invested in self-protection. According to Equation 10:

$$P^*(x) = \min_{\forall \bar{t} \in T[n_t][x]} ((\bar{F} \cdot \bar{t}) \times \bar{L}). \tag{11}$$

Then, we can simplify Equation 7 as:

$$\min_{\forall x} (P^*(x) + x). \tag{12}$$

Consider some amount of investments $x_r \in [0, W^0]$ to be evaluated at step $r \in [0; W^0/C]$. We are interested only in the following future steps p:

$$x_r + P^*(x_r) > x_{r+p} + P^*(x_{r+p}); \tag{13}$$

$$x_{r+p} < P^*(x_r) + x_r - P^*_{min}; \tag{14}$$

$$P^*_{min} = \bar{F} \cdot \left[\prod_{\forall k \in K} \bar{\pi}(k) \right]) \times \bar{L}. \tag{15}$$

Out of these two relations we can derive the following observations. First, Equation 13 shows that we should select the optimal value by iterating sequential comparison of the current best value (i.e., up to step r) with the next ones ($p > 0$). Equation 14 tells us the maximal steps we should look forward, since no more efficient total expenditure is possible for the steps higher than this limit. Finally, we also may find the first limit, which is: $x_0^{limit} = P^*(0) - P^*_{min}$, where P^*_{min} is the minimal possible premium/risk, computed with all possible countermeasures $K_i = K$ installed.

It is also important to note, that once we find a better x, we can re-set the limit, since it will be less than the previous one. This observation can be easily proved as follows. Let x_r be the previous best value (i.e., for all $r + p - 1$ steps) and x_{r+p} be even better than x_r, i.e.,:

$$P^*(x_r) + x_r > P^*(x_{r+p}) + x_{r+p}. \tag{16}$$

The limits defined at steps r and step $r + p$ are x_r^{limit} and x_{r+p}^{limit} consequently:

$$P^*(x_r) + x_r - P^*_{min} = x_r^{limit} \; ; \quad P^*(x_{r+p}) + x_{r+p} - P^*_{min} = x_{r+p}^{limit}. \tag{17}$$

We conclude that $x_r^{limit} > x_{r+p}^{limit}$.

3.4 Algorithm for computation of optimal self-investments

Now, we are able to define an algorithm for finding the optimal amount of investments x^*, which is based on the dynamic programming approach for solving 0-1 multi-objective knapsack problem. *Although, we use the core part of the well-known algorithm, we adapt it to our task: instead of receiving the limit for investments as an input, our algorithm should return it as an output, ensuring that it is the most optimal amount of investment.*

Algorithm 1 Selecting the best set of countermeasures

1: **procedure** searchForOptimalInvesments(K, c, π, $\bar{F}$, $\bar{L}$, x_{init}, $\bar{pr}_{init}$, C)
Require: K ▷ - a set of countermeasures
2: $c : K \mapsto \mathbb{N}$ ▷ - cost function
3: $\pi : K \mapsto 2^{[0;1]}$ ▷ - survival probability per threat function
4: $\bar{F}$ ▷ - frequency vector of $\mathbb{R}^+$ values
5: $\bar{L}$ ▷ - single loss expectency vector of $\mathbb{N}^+$ values
6: $x_{init} \in \mathbb{N}$ ▷ - initial investments
7: $\bar{pr}_{init}$ ▷ - initial overall probability of survival vector of values from $[0; 1]$
8: $C \in \mathbb{N}$ ▷ the greatest common divisor for countermeasure cost
Ensure: `lowest` $(\bar{F} \cdot \bar{pr}(K_i|x)) \times \bar{L} + x$ `for optimal security investment` x^*
9: $exp \Leftarrow (\bar{F} \cdot \bar{pr}_{init}) \times \bar{L} + x_{init}$ ▷ Remember the initial expenditure as optimal
10: $P^*_{min} = \bar{F} \cdot \left[\prod_{\forall k \in K} \bar{\pi}(k)\right]) \times \bar{L}$
11: $x^* \Leftarrow 0$ ▷ Optimal Investment starts with x_{init}
12: $\forall j\ T[j][0] \Leftarrow \{\bar{pr}_{init}\}$ ▷ a dynamic matrix of optimal probabilities. Add new (and the first) column $x = x_{init}$, with just one vector $\bar{pr}_{init}$
13: $x \Leftarrow C$ ▷ the size of set K
14: $n_k \Leftarrow |K|$
15: **while** $x + x_{init} \leq exp - P^*_{min}$ **do** ▷ Do while x is below the optimal expenditure
16: $\forall j\ T[j][x] \Leftarrow \{\bar{pr}_{init}\}$ ▷ Add new column x, initialised with vector $\bar{pr}_{init}$
17: **for** $j \Leftarrow 1, n_k$ **do** ▷ for all countermeasures
18: **if** $(c(k_j) \leq x\ )$ **then** ▷ check the cost limit
19: $T[j][x] \Leftarrow non - dominant \begin{cases} \bigcup\limits_{\forall l} \bar{\pi}(k_j) \cdot T[j-1][x - c(k_j)][l] \\ T[j-1][x] \end{cases}$ ▷ store all non-dominant vectors comparing two sets: with new control and without.
20: **else**
21: $T[j][x] \Leftarrow T[j-1][x]$ ▷ continue without adding new control j
22: **end if**
23: **end for**
24: **for** $l \Leftarrow 0, |T[n_k][x]|$ **do** ▷ for all vectors stored in $T[n_k][x]$
25: **if** $(\bar{F} \cdot T[n_k][x][l]) \times \bar{L} + x + x_{init} < exp$ **then** ▷ reduced the expenditure?
26: $exp \Leftarrow \bar{F} \cdot T[n_k][x][l]) \times \bar{L} + x + x_{init}$ ▷ Store this expenditure as optimal
27: $x^* \Leftarrow x$ ▷ Remember these investments as optimal
28: **end if**
29: **end for**
30: $x \Leftarrow x + C$
31: **end while**
32: **return** $[exp, x^*]$
33: **end procedure**

In the Algorithm 1, we demonstrate the core part of our solution which: a) finds the optimal investments in self-protection x^*; b) ensures the lowest expenditure $((\bar{F} \cdot \bar{pr}(K^*_i|x^*)) \times \bar{L} + x^*)$.

We start with all initial variables and functions provided. Moreover, we assume that the company has already some countermeasures K_{init} installed, spending already x_{init} amount of money and getting the initial overall probability of survival equal to $\bar{pr}_{init}$. Note that it is not important if the initial countermeasures K_{init} are efficient or they are not, but these controls should not be considered in the further analysis: $K_{init} \cap K = \emptyset$.

Lines 9-14 initialise the values for further processing. First, we store the initial expenditure and find the minimal premium P_{min}. We also initialise the auxiliary table of probabilities T with the initial column for additional investments $x = 0$ (the first column) and with all cells initialised as $\{\bar{pr}_{init}\}$ (Line 12). There is no need to compute values for $x = 0$ as no countermeasures could cost less than or equal to 0, i.e., $\forall j(c(k_j) > x = 0)$; so, we start with $x = C$, where C is some fixed greatest common divisor for the cost of all controls.

We are going to increase gradually the investments unless we reach the limit set by parameter $exp - P_{min}$, as Equation 14 states (line 15). For all countermeasures (line 17), we select all non-dominating overall survival probability vectors by comparing two sets: 1) a set of previously selected controls with k_j ($\bigcup_{\forall l} \bar{\pi}(k_j) \cdot T[j-1][x - c(k_j)][l]$), 2) and the best selection of controls without k_j ($T[j-1][x]$)(line 19). We should note here that both compared sets contain non-dominant vectors (as ensured at the previous steps), but two vectors from different sets could be dominating and dominated.

Since we use a modified knapsack problem, we multiply values when adding new countermeasure to the selected set, rather than summing values as the classical knapsack problem does. Note that we must respect the additional self-investments x, so the contribution of the considered countermeasure k_j is added to overall probability of survival computed for self-investment limit $x - c(k_j)$. Naturally, if the cost of the countermeasure k_j ($c(k_j)$) is higher than the additional self-investments x (line 18), we simply take the previously selected set of countermeasures and the corresponding overall probability of survival is $T[j-1][x]$ (line 21).

When all countermeasures are considered for the current self-investments x, we use Equation 13 to check if the newly computed overall amount of expenditure is lower than the previous one (line 25). Here we would like to remind that a cell of matrix T contains a *set of vectors*, i.e., we should evaluate all of them ($T[n_k][x]$). If the best current expenditure is lower than the previous optimal one, we set the current value as a new lowest expenditure and as the new limit (line 26) for further computations (according to the condition in Equation 14), plus we remember the current self-investments x as optimal x^* (line 27).

Algorithm 1 stops when further increase of the self-investments x becomes so inefficient that it exceeds overall best-so-far expenditure exp (line 15), i.e., the current optimal total expenditure for both insurance ($P^*(x^*)$) and self-investment (x^*). As a result, the algorithm returns the optimal self-investment limit x^* and the optimal total expenditure. With a slightly modified standard backward algorithm it is also possible to find the most efficient set of countermeasures K_i^*.

4 Case study

As a case study, we consider an organisation with initial wealth $W^0 = 100000$ which decides how to distribute the available funds to reduce cyber risks. First, five main threats are identified, as well as their average frequency ($\bar{F}$) and single loss expectancy ($\bar{L} = \langle 3000, 1800, 2800, 4000, 3800 \rangle$). So far, only the basic cyber security countermeasures are implemented (with the total initial investments ($x_{init} = 200$) and initial probabilities of survival $\bar{pr}_{init}$) but an analyst has identified eight additional countermeasures which can be installed ($|K| = n_k = 8$), their relative costs ($c(k_1) = 480;\ c(k_2) = 240;\ c(k_3) = 120;\ c(k_4) = 80;\ c(k_5) = 200;\ c(k_6) = 120;\ c(k_7) = 280;\ c(k_8) = 200$) and the probabilities of survival ($\bar{\pi}$ function). All input vectors are defined in Table 2.

$\bar{pr}_{init}$	$\bar{F}$	$\bar{\pi}_{k1}$	$\bar{\pi}_{k2}$	$\bar{\pi}_{k3}$	$\bar{\pi}_{k4}$	$\bar{\pi}_{k5}$	$\bar{\pi}_{k6}$	$\bar{\pi}_{k7}$	$\bar{\pi}_{k8}$
0.6	0.8	0.3	0.9	0.5	0.8	0.9	0.8	0.8	0.6
0.7	0.5	0.2	0.8	0.7	0.6	0.5	0.7	0.1	0.7
0.8	0.4	0.5	0.9	0.9	0.9	0.8	0.5	0.4	0.5
0.6	0.7	0.7	0.2	0.8	0.8	0.6	0.8	0.9	0.8
0.6	0.5	0.3	0.7	0.6	0.2	0.5	0.6	0.8	0.5

Table 2. Input vectors

If we apply our approach based on the dynamic programming proposed in Section 3.4, we start with initial expenditure *exp* equal to 5986. This expenditure will be our first limit for searching the optimal investment level. Naturally, $\bar{pr}(K_i|x))$ equals to vector $\bar{pr}_{init}$ in the beginning. The minimal premium is equal to $P^*_{min} = 136$. Table 3 contains the result for the first 21 rounds of the algorithm. In the first round, our expenditure increases by the investment increment $C = 40$

x	0	40	80	120	160	200	240	280	320	360	400	440	480	520	560	600	640	680	720	**760***	800
exp	5986	6026	4188.4	4228.4	4268.4	3178.4	3213.5	3028.2	2471.1	2511.1	2422.3	2334.1	2310.6	2036.7	1879	1919	1845.7	1861	1812	**1642.2**	1682
K_i	0	0	4	4	4	3,4	3,6	4,8	3,4,6	3,4,6	3,4,8	2,3,4	2,3,6	3,4,6,8	2,3,4,6	2,3,4,6	2,3,4,8	2,3,6,8	3,4,5,6,8	**2,3,4,6,8**	2,3,4,6,8

Table 3. Selection of best countermeasures within security investment

since there are no countermeasures of the cost below the current investment level $x = 40$. After the first two rounds of investment ($x = 2 * C = 80$), we find a possible solution, if countermeasure k_4 (with $c(k_4) = 80$) is selected (overall expenditure *exp* becomes 4188, which is lower than previous limit 5986). Thus, we raise the current optimal value of X^* to 80. The next increment of x ($x = 120$) increases the expenditure up to 4228 and we see that there is no more efficient countermeasure set than previous choice $\{k_4\}$. As we continue the analysis, we see that, although, in general, the overall expenditure falls, in some cases (e.g., for

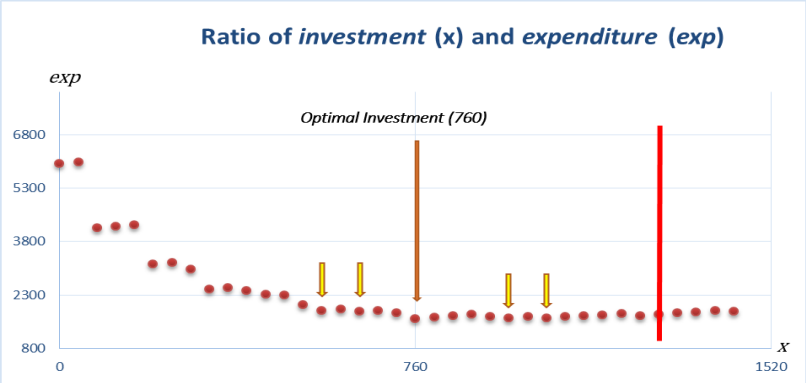

Fig. 1. (Exp) expenditure for security self-investments x

$x = 80$, $x = 320$ or $x = 560$), it raises. Thus, it is obvious, that our problem may have local minimums, but the algorithm easily overcomes them and continues up to the global minimum. The intermediate results of our algorithm, with several local and one global minimums, are displayed in Figure 1. The global minimum (optimal self-protection investments) is found at $x^* = 760$, with $exp = 1642$ and the set of selected countermeasures $\{k_2, k_3, k_4, k_6, k_8\}$. After finding the optimal value, our algorithm continues up to $x = 1642 - 200 - 136 = 1306$. Although some values of investment have got close to the optimal value (e.g., for $x = 960$ and $x = 1040$), non of them becomes a new optimum and the algorithm stops (red vertical line in Figure 1). Note that initially we planned to check the self-investment values up to 5986, but eventually stopped at $x = 1280$, preventing the unnecessary computational resource usage.

5 Related work

Cyber insurance is a young market which slowly matures facing a number of challenges [5, 22, 4]. Some of these challenges (e.g., lack of data, definition of contractual language, specification of standards for cyber insurance underwriting process) are of practical nature and mostly require insurers to gain more experience in the field. On the other hand, such challenges as correlated risks, interdependent security and information asymmetry require careful theoretical analysis in order to help the market to flourish and the society to benefit from it.

One of the central problems considered by several researchers is proving that availability of insurance incentivises agents to invest more in self-protection [6, 8, 13, 15]. Many well-known cyber security researchers believed that this is true [24, 9, 10], but a thorough mathematical analysis has proved that sometimes agents may simply decide to insure the future losses rather than increase their protection [13, 16], especially if interdependent security and information asymmetry take place [8, 13, 15, 11]. Thus, researchers considered various regulatory

mechanisms which can ensure high enough investments in self-protection and acceptable cyber insurance contracts: fines and rebates [8, 12], liability coverage [13], non-competitive market [14]. For performing these analysis, the researchers applied two types of models for modelling the relation between investments and the probability of attack: 1) a continuous model, decreasing the probability with any investment [8, 13, 15]; and 2) a simplistic discrete model, allowing two levels for the probability (high and low), depending on whether investments exceed a threshold or they do not [6, 12]. In contrast to these papers, we propose a more realistic model which increases protection only when enough investments for installation of the next countermeasures are available and allows as many of such increases as required. We have shown how the probability of survival (or a probability of attack) could be computed using a set of available countermeasures, and how the investments could be distributed between the self-investment and cyber insurance. One may argue that the continuous model is just an approximation of the reality, which skips the low-level details for the sake of simplicity of the more complex analysis. This may well be true, but then our approach could be seen as the link between the low level details and high level model, as well as the instrument for proving that such approximation is valid.

The problem of selecting the right set of countermeasures for cyber security is not new. For example, T. Sawik [18] conceptualises the selection of countermeasures based on their efficiency of blocking threats and cost of countermeasures. For doing this, he applies single- or bi-objective mixed integer program and conditional value-at-risk approach. The variety of knapsack problems [20] and their solutions are natural choices for being applied in optimisation of cyber security. For example, F. Smeraldi et. al., [17] introduced a framework which combines combinatorial optimisation with classical Knapsack Problem in order to spend security investment optimally. A. Fielder et. al., [19] investigated both game theoretic and Knapsack approaches for efficient security investment in Small and Medium Enterprises (SMEs). L. Krautsevich et. al., [21] applied the 0-1 knapsack problem to selection of the most secure web-service. In contrast to these papers, we considered the problem of minimisation of the probability of survival, adapting the problem to the 0-1 multi-objective knapsack problem. But, it is more important to note that were looking for the optimal specification of the investment limit, which is the input to classical knapsack problems. In short, we did not simply applied the knapsack problem to our scenario, but have solved a different problem (i.e., defining the optimal investment in self-protection and insurance) using the solution of the knapsack problem only as its integral part.

6 Conclusion

In this paper, we have proposed a viable solution for maximising the utility of an organisation by finding an efficient distribution of investments in self-protection and cyber insurance. In contrast to the exiting models used for the definition of such distribution, we applied a discrete model of self-investments which allows selecting concrete countermeasures that efficiently protect the organisation and

reduce the insurance premium. For selection of countermeasures we applied a solution based on the 0-1 multi-objective knapsack problem, but our solution goes beyond this well-known problem and looks for efficient investments (which is a prerequisite for the knapsack problems). The algorithm developed on the theoretical background ensures that only the minimal amount of evaluation cycles are executed.

Not only does our model provide a more practical approach for investment distribution and helps to select the concrete countermeasures to install, but it is also able to conduct the analysis of the planned configuration which is not 100% efficient from security point of view. Such configuration could be enforced by the global enterprise rules, Service Level Agreements or by the law (e.g., GDPR). Although the enforced configuration may be not the most efficient, it still reduces the probability of threat survival and cannot be ignored in the analysis (especially, because it has its own cost).

So far, this paper mostly focuses on the modelling of investments. In contrast to other models, we did not analyse how discrete investments affect the incentive of insureds to invest in self-protection with and without insurance. We also did not include security interdependence and information asymmetry problems into our model. These future steps are required in order to make more precise (and practical) predictions about cyber insurance market behaviour.

References

1. Symantec: Internet Security Report. Volume 22, 2017.
2. Cisco: Annual Cybersecurity Report, available via http://www.cisco.com/go/acr2017, 2017.
3. PartnerRe: Survey of Cyber Insurance Market Trends. available via https://partnerre.com/, 2017.
4. A.Marotta, F.Martinelli, S.Nanni, A.Orlando, A.Yautsiukhin: Cyber-insurance survey. Computer Science Review 24, 35–61 (May 2017)
5. ENISA: Incentives and barriers of the cyber insurance market in europe, available via http://www.goo.gl/BtNyj4 on 12/12/2014, June 2012.
6. 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.
7. Bazgan, Cristina, Hadrien Hugot, and Daniel Vanderpooten. "Solving efficiently the 01 multi-objective knapsack problem." Computers & Operations Research 36, no. 1 (2009): 260-279.
8. 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)
9. R.Anderson, R.Böhme, R.Claytin, T.Moore: Security economics and the internal market, January 2008.
10. R.P.Majuca, W.Yurcik, J.P.Kesan.: The evolution of cyberinsurance. The Computing Research Repository pp. 1–16, 2006.
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,. pp. 145–154. ACM, 2014.

12. Z. Yang, J.C.S. Lui, Security adoption and influence of cyber-insurance markets in heterogeneous networks, Perform. Eval. 74 (2014) 1-17.
13. 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.
14. 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.
15. 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)
16. 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.
17. 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.
18. Sawik, Tadeusz. "Selection of optimal countermeasure portfolio in IT security planning." Decision Support Systems 55.1 (2013): 156-164.
19. Fielder, Andrew, et al. "Decision support approaches for cyber security investment." Decision Support Systems 86 (2016): 13-23.
20. Bartholdi III, John J. "The knapsack problem." Building Intuition. Springer US, 2008. 19-31.
21. 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.
22. C. Biener, M. Eling, J. Wirfs, Insurability of cyber risk: an empirical analysis, (2014).
23. Rothschild, Michael, and Joseph Stiglitz. "Equilibrium in competitive insurance markets: An essay on the economics of imperfect information." In Uncertainty in economics, pp. 257-280. 1978.
24. Schneier, Bruce. "Insurance and the computer industry." Communications of the ACM 44, no. 3 (2001): 114-114.