UNIVERSITÀ DEGLI STUDI
DI TRENTO

DEPARTMENT OF INFORMATION ENGINEERING AND COMPUTER SCIENCE
IECS Doctoral School

Relation between cyber insurance and security investments/controls

Cyber Security Expenditure Distribution Framework

Ganbayar Uuganbayar

Advisor

Prof. Fabio Massacci

Università degli Studi di Trento

Co-Advisor I

Prof. Fabio Martinelli

Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche

Co-Advisor II

Dr. Artsiom Yautsiukhin

Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche

March 2021

Abstract

Nowadays, organisations consider cyber security risk as one of the critical risks at organisations. Due to the increase of cyber-related attacks and more advanced technologies, organisations are forced to implement the proper cyber risk management and find the optimality of security expenditure distribution for treating those risks.

About twenty years ago, cyber insurance has been introduced as one of the risk treatment methods backing up the security controls. The concept is further benefiting both organisations and the market, where the insurers globally expect 20$ billion in 2025 [1]. On the other hand, cyber insurance has been dealing with several hurdles on the way to maturing. One of the problematic challenges is the relation between cyber insurance and security investments (or controls). Several papers theoretically devoted the analyses on this issue where some highlighted that cyber insurance could be an incentive for security investments while others claim may lead to the fall of investments for self-protection. Since everything lies in a densely interconnected and risk-prone cyber environment, there are various factors on the relation, which effects should be thoroughly investigated.

The overall goal of the thesis is to analyse the problems lying in the risk treatment phase and propose an applicable solution to deal with. In particular, we would like to take into account the following factors to address the relation between cyber insurance and security investments. We first analyse different market models to study possible ways to keep both cyber

insurance and security investments in both competitive and non-competitive insurance markets. Some studies showed that security investments fall in the non-competitive insurance market. In this regard, we would like to investigate the possibility of raising the security investments by optimising the loading factor, an additional amount of fee for the premium.

In practice, organisations do not face a single threat but multiple-threats during a certain period. To the best of our knowledge, there is not a study considering multiple threats in the cyber insurance field to analyse how security investments can be varied. Thus, we investigate the multiple threats case in a competitive cyber insurance market and find how security expenditure can be efficiently distributed between the insurance premium and security investments/controls. The analysis allows us to map security controls and cyber insurance cost-effectively. We provide both theoretical and algorithmic solutions to deal with the problem and validate the solutions in both artificial and practical cases. For a practical scenario, we develop a questionnaire-based risk assessment tool to feed our risk treatment solution with necessary empirical data.

In both insurance markets, a degree of security interdependence is a unique peculiarity that affects the behaviour of organisations to invest in their self-protection and have cyber insurance. We theoretically analyse the effect of security interdependence in both market models and show whether it affects positively or negatively.

Keywords

[Cyber insurance, Security investments, Risk treatment, Security control selection, Optimisation of security expenditure]

Contents

List of Tables

List of Figures

List of Publications

1. Ganbayar Uuganbayar, Artsiom Yautsiukhin, Fabio Martinelli, and Fabio Massacci. "Optimisation of cyber insurance coverage with selection of cost effective security controls." Computers & Security (2020): 102121.

2. Fabio Martinelli, Albina Orlando, Ganbayar Uuganbayar and Artsiom Yautsiukhin. "Preventing the drop in security investments for non-competitive cyber-insurance market." In International Conference on Risks and Security of Internet and Systems, pp. 159-174. Springer, Cham, 2017.

3. Ganbayar Uuganbayar, Artsiom Yautsiukhin and Fabio Martinelli. "Cyber Insurance and Security Interdependence: Friends or Foes?." In 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), pp. 1-4. IEEE, 2018.

4. Ganbayar Uuganbayar, Fabio Massacci, Artsiom Yautsiukhin and Fabio Martinelli. "Cyber Insurance and Time-to-Compromise: An Integrated Approach." In 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), pp. 1-8. IEEE, 2019.

5. Fabio Martinelli, 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.

Acknowledgement

- The path toward this thesis was an incredible journey of learning, failing, improving and creating. My genuine gratitude goes to Professor Fabio Massacci, who advised me to enrol for the PhD at the University of Trento under his supervision. His profound knowledge in cyber security and the academic field unequivocally helped me to learn a lot, and more importantly, his support was exceedingly abundant.

- If it were not for Professor Fabio Martinelli and Artsiom Yautsiukhin, I would not have had a chance to grasp this opportunity from the beginning. They believed in me to be a part of the European Cyber Security project titled "NeCS" and become a researcher at the National Research Council (CNR). I am genuinely grateful for my supervisors and colleagues at the National Research Council of Italy. "2 socks + 3 ideas + 21 ants = 111 litres of water" was one of the comments by Artsiom on my first paper. This is how he taught in such a way that I never forget.

- A true friend is hard to find and impossible to forget. During my study, there were times when I was struggling a lot and staying nights without sleeping. Usukhbaatar Dotgonvanchig, my best friend, tremendously helped me to overcome the challenges. I am indebted to my friend whose value only increases as time goes.

- I am so lucky and proud that I worked with incredible colleagues (Christina, Oleksii, Athanasios, Claudio) who started the journey together at CNR and became an important part of my life. Not only

did we help each other in terms of work, but we also supported each other for life. We are bound to be life-long friends.

- Living abroad alone was not an easy task until I met some enthusiastic guys (we call ourselves as "Meet Up, Keep Fit, Make Friends or HiRunDo" group). I am always energised and refreshed when we meet and do so many different activities, i.e., hiking, training and cooking. You are always welcome to visit my home country, Mongolia, and always be friends.

- My deepest and dearest appreciation belongs to my family and friends for their support, understanding and love. Without them, I am just a whisper of nothing.

- Last but not least, I would like to thank prof. Andrea Pugliese and prof. Silvia Bonomi for reviewing my thesis work. The reviews were incontrovertibly helpful to improve the thesis.

Chapter 1

Introduction

"It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it" – Stephane Nappo. Cyber security, especially these days, is being considered as one of the crucial topics since more organisations and individuals are being targeted by different types of cyber attacks [2, 3, 4]. There are numerous motivations behind the growth of cyber attacks, such as rapidly changing attack surface, emerging advanced tools and lack of security awareness campaigns [5, 6]. The resulting losses have already made the organisations consider cyber risks to be an essential part of their whole risk management. For example, Wanna-Cry Ransomware attack[1] [4] caused globally a huge loss equal to 4$ billion and hit around 230,000 end devices in 150 countries.

Moreover, the dynamicity of cyber security landscape is noticeably and rapidly changing. Especially, in the last years, many end devices are on the rise and the interconnectedness of the cyber world is becoming more complex due to IoT and Cloud trends. From the perspectives of usefulness and efficacy, these advanced technologies are bringing various advantages into our daily life. On the other hand, Symantec reports [2, 3] highlighted that many security breaches in IoT are on the rise comparing to past years. Last but not least, Ponemon and IBM [7] reported insights on the financial

[1] A type of attack which encrypts all data, i.e., pdf files, and asks for a ransom to decrypt.

impact of cyber attacks and corresponding mitigation controls. The report underlines how severe cyber attacks can be and having mitigation controls is not a sufficient defence mechanism. In summary, cyber risks and attacks are proliferating irrespective of current approaches, and it is required to have other (up to date) treatments of these risks as a simple mitigation technique cannot solely solve the problem.

To deal with these challenges, from a senior management perspective, the first and the foremost action is to implement proper cyber risk management, which involves different personnel from various fields of the organisation. Depending on the type of organisations, there are numerous guidelines, standards and policies to follow in terms of managing the risks. Cyber risk management is effective when it complies with the right (sometimes mandatory) policies and standards alongside.

In general, the risk management process comprises three core steps – 1) *assessing and analysing* the risks, 2) *treating* those identified risks and 3) *reporting, monitoring and updating [23, 98].* However, considering different factors (i.e., advanced hacking technologies) in cyber security, the cyber risk assessment process has always been challenging. This eventually results in an inefficient security investment strategy during the risk treatment phase. Moreover, a limited budget and scarce information on security posture make the risk treatment process considerably complicated and erroneous. Regardless of obstacles, risk assessment is the pivotal activity to efficient risk management implementation and it enables the possibility of linking technical aspects and high-level models.

1.1 Risk Assessment

Risks, in general, are related to potential future incidents and their likelihood of being occurred. Thus, the risk is considered as a result of proba-

bilistic[2] events. To manage and measure those risks, risk assessment plays a vital part, which helps to find the likelihood of certain attacks (or incidents) and the resulting impact on a condition that the attackers achieved their goal. The whole process comprises identifying the assets, threats and vulnerabilities for either qualitative or quantitative analysis. So far, numerous approaches were proposed, i.e., MAGERIT [12] and others [8, 13, 20], to identify and an accurate assessment process for analysis of cyber risks. The risk identification phase defines the assets, threats and vulnerabilities that should be treated.

From the risk assessment team side, the most basic and simple method to obtain the information on the risk identification phase is to conduct meetings and interviews with stakeholders [12, 8, 13]. Even though these approaches may provide us with full information about the security level, they are considered time-consuming and sometimes inaccurate because of practitioners' lack of expertise (i.e., most SMEs do not have a dedicated expert on dealing with security issues). To support the information collection processes, questionnaires, i.e., ISRAM by Bilge Karabacak et al., [14, 15] are widely adapted and they are often created based on well-known security standards. Other technical methods, such as network scanning, further appear to be incredibly useful for the identification phase. Based on the information found, an assessment team continues with the analysing phase to determine how likely identified vulnerabilities can be exploited and what is the expected impact once it is being exposed. The analysis phase can be conducted in either a quantitative or qualitative manner. In practice, a combination of methods is often recommended since they have their advantages and disadvantages.

An important but difficult part is to accurately find the likelihood of attack (or a successful threat occurrence). In practice, this likelihood can

[2]Cyber security incident may happen or not

be determined using internal statistical data or taking data from global surveys, like the ones from Symantec, Ponemon, etc [7, 2]. Unfortunately, often internal statistics is not enough to identify these likelihoods and global surveys are not organisation-specific. Several scientific authors [13, 12, 16] tried to approach this problem by adapting Attack Trees and Graphs to compute the probability of being compromised and suggest applicable countermeasures at each phase. Mcqueen et al., [17] proposed a time-to-compromise metric to find the likelihood of attack based on obtainable information in vulnerabilities and exploits. The idea was extended by [19] with consideration of CVSS value. Also, F.Massacci et al., [20] introduced a model to estimate the organisation's likelihood of attack quantitatively by having consideration of two attack phases. Their methodology is based on actual data that can be accumulated through Intrusion Detection System (IDS) and periodic Vulnerability Assessment (VA) for any organisations.

In this work, we adopt the idea of the questionnaire approach to obtain the basic information to identify and analyse the organisation's risk. The questionnaire risk assessment process helps to identify all available and installed security controls so that our risk treatment solution can be fed. Not only do we adapt the concept of questioning, but also we extend the method by applying the weighted approach (weighting all contributions of vulnerabilities/protections for specific threats) and the time-to-compromise metric as an alternative way to assess the risk. The result of the approach can help us to find the likelihood of attack and knowledge on the organisation's security posture.

1.2 Risk Treatment

Once cyber risks are assessed and evaluated, the next step, the risk treatment process, should be carried out. Also, it is worth mentioning that the

main focus of the thesis work has been done in the risk treatment phase. This step includes the following alternatives – 1) *risk mitigation* by installing security controls, 2) *risk transfer* by shifting the full or partial losses to a third party (i.e., cyber insurance), 3) *risk avoidance* by withdrawing from the risky activity and 4) *risk acceptance*, which, an organisation simply accepts the residual risk. Basically, an organisation should devise an efficient approach to make a rational decision on whether to reduce, transfer, accept or combine the methods. According to available surveys, there is always the residual risk even though organisations are confident enough for their security controls[3] [6]. This indicates that having a mitigation solution solely does not treat the risks as one desires. So, the combination of risk treatment options are highly recommended but should be carried as efficient as possible. The main challenge in the risk treatment phase is to allocate the security expenditure in a cost-efficient way.

Security expenditure distribution for risk treatment options is a challenging topic among researchers and practitioners since cyber security comprises a vast area including both technical topics and mathematical models. To know the efficacy of security controls, Gary Stoneburner et al., [23] and Gordon et al., [22] conceptualise the cost-benefit analysis which shows the benefits in saved expenditure because of installation of security control. In practice, Return on Security investments (ROSI) [24] analysis is a viable approach since it considers each controls separately and eventually aggregates the results for an analyse. Moreover, when other treatment options are considered, there is a need for more generic analysis.

In this work, we thoroughly investigate the security expenditure distribution problem among risk treatment options and propose the applicable solutions to deal with the identified challenges. The concepts are detailed in the following sections.

[3]Security controls can be either/both administrative, technical and physical to protect the assets.

1.3 Cyber Insurance

To support the risk mitigation option, cyber insurance, a risk transfer alternative, has emerged in past decades to alleviate the financial losses. The market is flourishing even though the pace is not as it was expected [25, 1]. Apart from the market view, the impact of cyber insurance on security perspective has been studied by numerous researchers and practitioners, i.e., Jean Bolot et al., [27] and others [28, 29, 30, 32, 33]. Depending on the taken assumptions, the effect of cyber insurance varies – some papers underline that it wears-off the losses while others, i.e., Massacci et al., [32] pointed out that cyber insurance might create problems by eroding security investments. On the other hand, both insurers and insureds can benefit from the impact of cyber insurance where an organisation/insured strengthens the security by transferring the residual risks [25].

In particular, cyber insurance has been dealing with a specific problem, which is – its impact on security investments for one's self-protection. Some researchers, i.e., Bruce Schneier [36] and others [39, 40], found out that cyber insurance can be an incentive to invest for the self-protection, while H.Ogut et al., [35] and others [34, 38, 27], claimed that once an organisation has the cyber insurance option, it may invest less or nothing for the ex-ante security controls. Various factors and assumptions influenced to yield different results, whether it is positive or negative. Cyber insurance market model, competitive[4] or non-competitive, is one of them. A distinction of the markets is that the non-competitive market adds an additional fee[5] for

[4] A general conceptual model which does not provide profit to an insurer but highly adaptable for a theoretical approach.

[5] An additional fee added for the premium from insured to the insurer, i.e. administrative cost.

the premium computation as:

$$Premium = Risk \quad - \textit{in competitive market;}$$
$$Premium = LoadingFactor \times Risk \quad - \textit{in non-competitive market}$$

This aforementioned process makes the investigation in the non-competitive market model more complex than it is done in the competitive market model [27, 48, 30, 35, 34]. On the other hand, the competitive market is considered as a formal and generic model according to Shetty et al., [43] and is not profitable.

Additionally, current cyber insurance literature considers only a single threat case for the models. In practice, this case is not always adapted since we deal with different types of threats and losses every day (e.g., see examples of threats from the ISO27005 standard [98]). Thus, current models find this difficult to conceptualise since the correlation between threats and security controls are complex. Also, there is a need for optimising the security investments for security controls which can decrease the insurance premium. For example, in [9, 96, 97], the authors identified potential threats and security controls in different systems, while an organisation may find it difficult to implement all required controls. To the best of our knowledge, the security control selection problem with the availability of cyber insurance option has not been investigated thus far. Especially, with the multi-threats case, no one has done the investigation on the relation of cyber insurance and security investment/controls in the competitive insurance market. Thus, our main goal is to investigate the identified challenges in the competitive insurance market model and propose an applicable solution.

To encourage the organisation to invest more in self-protection, several regulatory approaches were conducted, i.e. fine and rebate mechanism [27, 49, 38]. The mechanism additionally fines for insureds with low se-

curity and rebates for the ones with high security, next to discrimination strategy for assigning premiums. Also, an additional fee i.e., special tax, is another regulation mechanism and it usually appears in a non-competitive insurance market. Eventually, the premium is estimated higher than the competitive insurance market due to the added cost (so-called a loading factor) [25]. Several researchers, such as H.Ogut et al., [35] and Yang et al., [42] conducted a theoretical investigation on this market and how the market affects on insured's behaviour of investing for self-protection. The interesting point is to analyse if the loading factor can be considered as an incentive or positive regulator for self-protection or at least to avoid dropping security investment. We conduct our research considering this issue and propose a theoretical analysis for solving the problem.

A degree of security interdependence[6] is a unique factor in cyber security, especially in cyber insurance where several papers are devoted to the analysis of how it affects the insured's behaviour of investing for self-protection and having a cyber insurance alternative. H.Ogut et al., [35] and Zhao et al., [50] show that the increase of security interdependence leads to the drop in security investment. The problem is how much security interdependence affects security investments and cyber insurance in which way. In this work, we theoretically investigate the impact of security investments in both cyber insurance markets to find out how it affects under certain circumstances.

1.4 Contribution

The general goal of this thesis is to analyse the relationship between cyber insurance and security investments under various conditions. We have

[6] one's level of security does not depend on only its security investments but it is also affected by the partner's security investment.

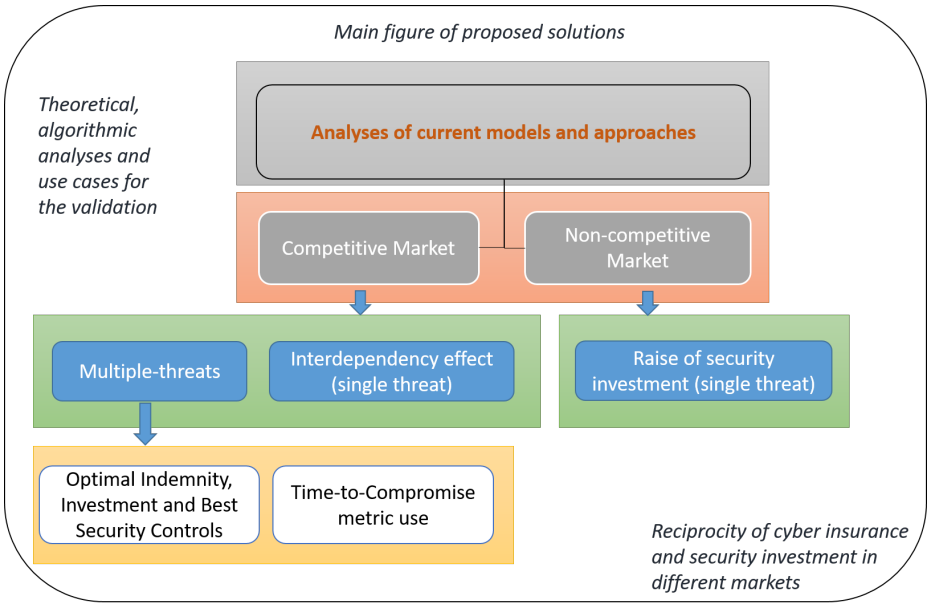


Figure 1.1: Main framework for the proposed solutions on the relation of cyber insurance and security investments in different markets with various factors

systematically reviewed over 500 papers on those topics in order for a conceiving fundamental analysis of the existing approaches and lying problems. The following Figure 1.1, shows the main insight of the proposed solutions and different factors which are covered: The proposed solutions will lie in two main parts, competitive and non-competitive insurance markets with a supporting investigation of security interdependence (which is considered as another chapter). The former section, which is the main research area of the thesis, helps a decision-maker to distribute the security expenditure in an efficient method between risk treatment options while the latter chapter, non-competitive market analysis, will prevent the security investments drop by optimising the loading factor. The first part, Chapter 3 is to deal with problems in a competitive insurance market of which its premium is actuarially estimated [25]. As a supporting part, the following, (Chapter 4) will be dedicated to validating our proposed solution in practical use cases. In this regard, we developed a questionnaire-based risk assessment tool

and integrated the tool with our proposed solution. Another approach is to compute the likelihood of an attack based on the time-to-compromise metric. Also, we theoretically investigated the impact of security interdependence in the competitive insurance market (see Chapter 5.2). Then, Chapter 6 will cover the problems related to falling security investments in a non-competitive insurance market.

The core contribution of **Chapter 3** is an approach for risk-averse[7] organisations to determine efficient security investments distribution between various risk treatment options (in particular for risk mitigation and transfer). Also, we determine specific security controls be applied. To the best of our knowledge, although the optimal selection of cyber security controls has been studied by many researchers, there is no study of mapping cost-effective security controls with cyber insurance. Our proposed solution helps organisations find the best set of controls with optimal security investments alongside the minimal insurance premium.

The second innovative aspect of our approach is considering multiple-threats in the cyber insurance model. The solution connects theoretical models with practical scenarios based on security controls and cyber insurance mapping notion. The crucial part of the solution is to investigate the problem in a discrete security investments model, in which, an organisation becomes capable of finding its security level and knowing what controls to install within their budget. We would like to highlight that we improved the traditional way of finding the best controls based on dynamic programming by applying projection idea. More importantly, not only an accurate algorithmic solution has been proposed, but also it was compared with approximate solutions, i.e., the Genetic Algorithm, for different settings. In summary, the main points are concluded as follows:

- a theoretical analysis of the distribution of the cost-efficient invest-

[7] a type of organisation that always attempts to reduce the risks.

ments when cyber insurance option is available,

- an explicit model to link security investments with selected security controls, assuming that some initially selected controls could be not optimal,
- a proposed exact solution for solving the optimisation problem (based on multi-objective knapsack problem) with new features,
- analysis of the proposed algorithms and approximate solutions (Greedy and GA), considering the effect of quantity and quality of inputs on the results.
- Mathematical prove that insureds prefer full insurance also in case of a multiple-threats case.

In **Chapter 4**, our proposed solution on an efficient security expenditure challenge is integrated with the risk assessment tool that we developed. Through the integration with the risk assessment tool, we delivered our risk treatment approach to a wider audience. In this way, the proposed solution helps organisations to deal with the security control selection process in practice.

In **Chapter 5.1**, we highlight a new way to look at the cyber insurance contract considering the Time-to-Compromise metric. Similar to travel insurance [51], we may change the duration of a cyber insurance contract by judging from their security level and time to be compromised by attackers. Although the proposed approach faces several challenges, it helps to link the low level (and potentially measurable and verifiable) time-to-compromise metric with the high-level risk value suitable for strategic decisions.

In **Chapter 5.2**, from a theoretical aspect, we have shown that cyber insurance is positively affected by a degree of interdependence. Our initial

analysis also showed that security investments can be raised when a cyber insurance option is available. It can be the base of further investigations.

In **Chapter 6**, we theoretically investigated the problem of security investment fall and showed how to raise it. We also underlined that insureds are still interested in buying some portion of insurance regardless of their high price. Also, the analysis involves the impact of security interdependence and how it affects the result.

Chapter 2

Related work

This chapter reviews the existing literature on cyber insurance and other related topics we investigated in the thesis. We systematically analyse the current approaches proposed by various authors in comparison with our solution.

Many public reports state, i.e., Cisco [6] that risk mitigation option solely is not best practice against cyber attacks. Cyber insurance was introduced two decades ago as a risk transfer option, and gradually contributing its impact to the cyber security area as it alleviates cyber-related losses. The cyber insurance market thrives globally, which expects 20 billion $ in 2025 [1]. Even though the pace is not as it was expected cyber insurers are still making profits, as well as insureds, are benefiting from the market. Also, both researchers and practitioners see cyber insurance as a promising alternative to deal with cyber incidents in such a way, which, insurers collect statistical data to use it for better estimation. Savino Dambra et al., [33] reviewed the existing approaches on how insurers estimate the premium and highlighted applicable recommendations. For instance, there is an urging need for more professionals to develop automatic-tools and data-driven solutions to replace the current qualitative approaches.

Furthermore, the cyber insurance premium can be seen as an indicator

to measure the security level of the organisation [25]. Sasha Romanosky et al., [46] conducted a qualitative analysis of revealing the crucial but often not public topics investigating the policies among insurance companies across the USA. The work searched for answers to What losses are covered? How they estimate the premium? and What type of questions are filled in to assess the risk?. The authors found that most insurers adapt the general (flat) equation to calculate the risks, while others use more sophisticated approaches incorporating different metrics. Also, there is a common confidence level among insurers, which indicates that they know what losses to cover and what to exclude. Despite the contribution, cyber insurance has been dealing with several challenges, which is broader than issues in traditional insurance scenarios. For instance, Shauhin et al., [47] analysed how the current cyber insurance market reflects on technology and what challenges should be considered. They further showed why governments should support insurers and maintain regulatory mechanisms.

In particular, as we have introduced in **Chapter 1**, the relation between cyber insurance and security investments is considered as one of the challenging problems [25]. The relation is further affected by different market models and other factors, such as security interdependence. For instance Arunabha Mukhopadhyay et al., [45] proposed Cyber-Risk Assessment and Mitigation (CRAM) framework to reduce the overall loss by decreasing the probability of successful attack and recommending complementary risk treatment options, i.e., cyber insurance. The authors adapted the generalized linear models (GLM) to compute the probability of attack by incorporating the idea of collective risk modelling to estimate the expected loss which can be mitigated through either security controls or cyber insurance. As a result, they recommend using cyber insurance when the probability of attack and impact is low. On the other hand, security controls are preferable to reduce the losses as a mitigation tool.

In this work, the core differences between the current approaches and our proposed solutions are illustrated in Table 2.1:

	Current approaches	**Our solution**
Competitive Insurance Market	Single Threat modelling	Multiple Threats modelling
	Mostly Theoretical Solutions	Both Theoretical and Algorithmic solutions
	No mapping of cyber insurance and security controls	Security control selection with premium
	High or Low level of security interdependence	Different level
	No study of TTC in cyber insurance	Integrated TTC metric
Security control selection	Selects the controls within the budget	Finds the optimal budget
	Use of simple examples	Complex cases and practical example
	No comparison between approaches	Proposed different approaches and compared
Non-competitive Insurance Market	Shows how security investment falls	Shows how to raise security investments by optimising a loading factor

Table 2.1: The core differences

In the following sections, we describe the existing solutions from different authors in detail and explain how our proposed solutions cover the gaps which are left unsolved.

2.1 Competitive Insurance Market

Cyber insurance market models can be seen as two main types, competitive and non-competitive depending on how it functions and estimates the premium [25]. We start our analysis in a competitive insurance market model because of its formality and less complexity for a conceptual investigation. Rotsch et al., [94] and Akerlof et al., [95] underlined that the competitive market model is considerably attractive than having a non-competitive model even though the competitive market does not make a profit without government regulation. Cyber insurance further derived the model as many researchers devoted their work to the competitive cyber insurance market model. In particular, the relation between cyber insurance and security investments is caught by various researchers [43, 30, 48].

In this work, we also focus on the same problem to study if there is an optimal trade-off between cyber insurance and security investments under certain circumstances.

Current papers cast the problem considering different factors and reached two main conclusions. Some researchers [36, 39, 40], i.e., Massacci et al., [32] claim that cyber insurance may trigger the security investments to fall and eventually organisations are inclined to invest less than it has no cyber insurance case. The result could be a higher premium which further depends on the organisation's security posture. On the other hand, others [35, 34, 38, 27], i.e., H.Ogut et al., [35] provide an analysis that shows that it is possible to keep both cyber insurance and security investments. Organisations/insureds could receive a lower premium if they harden their security. Arunabha Mukhopadhyay et al., [107] highlighted that an affordable premium is mapped to basic and concrete security controls. Also, insureds can be enforced to implement a baseline standard or compliance, such as GDPR [11] in Europe. The results varied due to the assumptions that the authors take into account.

One of the factors is the security investments model conceptualised by authors. It can be either continuous or discrete [25] investment model. In particular, H.Ogut et al., [35] and others [38, 34] investigated the correlation between security investments and the probability of attack by applying a continuous investment model which allows the fact that every investment decrease the probability of attack. The continuous model is often considered a high-level conceptual model which is widely used in theoretical analyses. On the other hand, the discrete investment model addresses the practical situation where not every investment is efficient due to overlapping security controls or costly ones. Jean Bolot et al., [27] and others [48] applied a discrete investments model, which can be seen as an oversimplified model considering a binary value for the probability (high or low),

depending on whether investments exceed a threshold or they do not. In a comparison with these papers, we have come up with a more realistic solution that allows the selection of the best security controls only when there is enough security investment available. The proposed approach enables the possibility of computing the probability of survival (or a probability of an attack) based on a set of available/selected security controls, and the method for how security expenditure is distributed between the cyber insurance premium and security controls (investments). Our approach can be seen as a bridge between high-level models (i.e., continues model) and low-level details, and the instrument for proving that such approximation is valid.

Furthermore, current papers on cyber insurance only model a single threat case which is not a practical case in real-world scenarios [25]. Organisations face many threats in which each of them can cause different losses (e.g., see examples of threats from the ISO/IEC 27005 standard [98]). Also, public reports and databases indicate that the organisation suffers different losses in a certain period [2, 3]. To close the gap, we cast the problem and propose our solution considering multiple threats. This unique challenge has not been investigated in cyber insurance by other researchers.

Although the effect of security investments has been theoretically investigated by many researchers [25], there is a limited study on how security controls are mapped to the premium estimation. In this work, to the contrast of many works, our main goal is to provide a thorough analysis for having cost-effective security controls and defining how to map them with the correlation of investments and probability. To the best of our knowledge, this problem has been avoided by researchers in past.

2.1.1 Security control selection

In past decades, selecting the best security controls received huge attention from various researchers. In particular, an enticement was to find the most cost-efficient approach. With the exception of a few, many existing works, i.e., [53, 56, 52], only provide theoretical analysis to the problem.

Among various approaches, Return on Security Investment (ROSI) [24], Attack Trees and Knapsack Problems [53] are mostly derived because of their adaptability and well-fit into the problem. For instance, Dewri et al., [56] and Chung et al., [52] combined Attack Tree and Return on Investment. In the former work, the authors presented a cost-benefit analysis against possible threats by maximizing the ROI index. As a supporting model, the attack tree was adapted and augmented with potential damage metric to correlate the dependency between security controls and vulnerabilities. They model attacker-defender interaction as an "arms race" and identify the security controls using multi-objective optimization and competitive co-evolution. The result shows that there are several advantages to catch, i.e. a quantitative approach of the problem, and yet it has a complexity which further increases with the population in competitive co-evolution. Chung et al., [52] proposed an interesting work to deal with cyber attacks in a virtual environment by selecting the best countermeasures from a predefined pool and adapting ROI to measure the effectiveness. The authors used an Attack Graph to model attackers and if there is a new vulnerability discovered or a countermeasure implemented, the graph will be updated. For the appropriate countermeasure selection, they used the graph in such a way as to decrease the probability of being compromised. Both above-mentioned works find the best controls within a predefined budget and compute losses for each threat which are aggregated afterwards. These cost-based analyses, which are partially showed in our greedy approach,

solve only the basic problem as opposed to ours where we find the optimal investment to invest.

In most cases, the security control selection can be seen as conceptual incorporation of two different representations of the control - cost and its ability to block the threats or close the vulnerabilities. T.Sawik [55] provided the solution based on the single- or bi-objective mixed-integer program. Same as other works, the author further finds the best security controls within a pre-defined budget (which is an input value to the program) by applying the Value-at-Risk (VAR) approach. The accuracy of the result depends on a decision-maker who selects the portfolio for integer programming through a commercial tool. Similar to the base concept of T.Sawik's work, other researchers derived the classic 0-1 Knapsack Problem (KP) [53] idea to solve the issue. Usually, this sort of problems is seen as NP-hard and optimisation solutions are often applied.

F.Smeraldi et al., [54] applied combinatorial optimisation, the original approach according to the authors, to Knapsack Problem to find an optimal security investment for the controls. The work shows another way to solve KP and particularly, it deals with multiple threats. Likewise to other existing works, it also takes the security budget as a criterion. Another work that used combinatorial optimisation is proposed by Andrew Fielder et al., [65], which integrated game theory analysis for the solution to capture the interpretation of attacker and defender. The main work is delivered in a theoretical approach and then applied to Small and Medium Enterprises (SMEs) for a validation purpose. The results they obtained was interesting at some points, particularly, concluded indirect cost has an impact on budget allocation and makes the decision-making more difficult.

Dynamic Programming To solve the Knapsack Problem, there are several methods provided by researchers. One of them is a Dynamic Programming

(DP) [66, 67] which finds the optimal selection through iterations until the certain condition meets. The solution is often lead to an exact answer but considered a time-consuming method when it deals with a large or complex input. In KP, the multi-objective context can be seen in different ways. Some researchers considered multiple objectives to set the criteria in KP. For instance, Bazgan et al., [68], proposed 0-1 multi-objective KP (considered 3 objectives for the experiment) has been solved by proposing dynamic programming, in which the authors used several complementary dominance relations at different states and conducted experimental validation. Another example of multi-objective KP is a Multi-Objective Tabu Search (MOTS) algorithm which was developed by Viduto et al., [60] to construct efficient non-dominated solutions. They propose a novel Risk Assessment and Optimisation Model (RAOM) to find the best countermeasures. However, their solution solves a slightly different problem which considers residual risk and security control objectives separately. It is worth underlining that multi objectives considered by other authors in multi-objective knapsack problem [54, 55, 56, 60] (minimisation of losses, minimisation of costs, maximisation of return of investments, etc.) are different than its meaning in our solution where it stands for multiple threats.

Greedy and Genetic Algorithm Since the performance of DP-based algorithms is proven to be time-consuming regardless of its accuracy, many researchers derived approximate algorithms to solve 0-1 KP. Evolutionary algorithms, i.e., Genetic Algorithm, or Greedy approaches are often considered in both literature and applications due to their capability of finding the optimal or nearest optimal solution within a much shorter time [69, 70]. Greedy approaches are considerably faster but often fails to provide the exact answer [76]. On the other hand, the Genetic algorithm shows some promising results even though it is not comparable with the

DP-based algorithm in terms of accuracy. GA has been improved by many researchers [101, 104, 71, 72, 61] to make the computation more accurate and efficient. It has been applied to various applications in real life, and more importantly in cyber security field. For instance, Suhail Owais et al., [73] conducted a survey to apply GA to Intrusion Detection Systems techniques, and Goranin et al., [72] adapted GA to find the countermeasures to mitigate the propagation of worms through the Internet.

Maya Hristakeva and Dipti Shrestha [101] proposed a GA-based solution for solving the 0-1 Knapsack Problem and compared two selection methods, roulette-wheel and group selection (they devised a name for their approach). As an outcome, they claim that the group selection with the elitism method outperforms the roulette-wheel selection in different cases, i.e., increasing the number of population. Another work to improve the accuracy of GA proposed by Gupta et al., [104] is a hybrid solution to create a better initial population. They applied "fcheck" function to the initialisation step to check whether the created population meets the criteria they set. The idea results from more good chromosomes in the population, which eventually improved the accuracy of the outcome. Also, Ahmad et al., [71] proposed a linear regression analysis for creating the most efficient and fit population, yet this work is dedicated to another problem, the travelling salesman problem (TSP). We have adapted some ideas of the aforementioned works to initialise the first population and improved them to fit into our work.

In [103], the authors applied the Genetic Algorithm to select the best countermeasures against specific threats. All variables for the model was considered as constant for the sake of simplification and they empirically experimented with their model. As a result, they find the most effective countermeasures against certain threats and the overall cost is within the specified security investment. However, this work does not provide an

exact answer to finding the best trade-off between security investment and expected risk. Considering only GA is not a salient example since it does not find the optimal solution in all cases. All GA solutions in Knapsack Problem only find the best or close to the best solutions within the budget, while we apply GA to a completely different problem where we find the optimal investment based on the best countermeasures.

Not only has the classic 0-1 Knapsack Problem been solved by GA, but also multi-objective KP is dealt with by GA [63, 61]. For instance, Kumar et al., [62] proposed an archive-based algorithm REMO (Restricted Evolutionary Multi-objective Optimizer), which uses the separate archive to store the remaining population-based on the restricted mating pool, while Jeffrey Horn et al. [64], introduced the Niched Pareto GA for solving the Pareto optimal population in multi-objective KP. However, we are not interested in multi-objective problem as they solved here since we are dealing with a different problem which has multiple threats.

The core difference between our proposed solution and existing approaches in finding the best security controls is that we adapted and improved (with a projection idea) the dynamic programming (DP) for the exact solution, and Greedy and Genetic Algorithm (GA) for the approximate solution, while others simply apply a generic model. For instance, [55] applied a mixed integer programming method to analyse a simple use case that only considers 10 threats and 10 controls (something, our algorithm can easily cope with). Smeraldi [54] further considered the classic dynamic programming and greedy algorithms, while we have also improved the DP with projection idea. Some authors [103, 56, 57, 61] adapted various evolutionary algorithms. On the other hand, our experiments prove that the improved GA is faster and reliable enough (with high settings), although it still may fail to produce the exact optimal answer. Furthermore, what makes our work unique and different in comparison with the

above-mentioned works is that we find the optimal security investment to spend on, while others consider the budget as if it is given in prior. Also, our model allows mapping security controls and cyber insurance in such a way that no one has done before. Even though some works contextualise the multiple threats case, this scenario has been avoided in the cyber insurance model so far. In this work, we analyse the gaps and propose our solution to close them.

2.1.2 Questionnaire-based RA tool

The most common method of obtaining information in risk assessment is to ask questions from stakeholders, experts and other managing parts through a course of meetings, workshops and interviews [12, 8, 13]. One of the well-known approaches is the Delphi method [82] which is helpful to improve the post-processing after the interviewing step. The process is consisted of two forms and performed by a small team that creates a questionnaire for participants [83]. When the participant/organisation fills the first form, the team analyse the questionnaire and send the second form. Also, analysis can be carried out through an automatic tool on condition whether all required questions are completed or left without filling.

To make information gathering easy, the checklists [84, 85, 86], and worksheets [8] can be integrated with questionnaire method [14] during the meeting and interview. Furthermore, these questions and checklists can be filled by an organisation or participant. We have adopted the notion of self-completion questions in our risk assessment tool which comprises different categories of questions dedicated to specific purposes.

The idea, questionnaire, is also adapted by Kruger and Kearney [87] to develop a method for measuring information security awareness of the organisation. The author used a basic data-processing approach for the gathered information and adapted a weighted approach combined with

certain multi-criteria problem solution techniques. Yeh et al., [88] further introduced a questionnaire-based method to study the correlation between security countermeasures and existing threats in the organisation. The questions are designed to empirically analyse the countermeasures adopted by the organisation and their effect on security perception. A similar method was adopted in a work of Nishioka et al., [89] to collect information on the organisation's way of hardening the security and more important way of designing the security. With adopting these ideas and approaches, we have developed an online risk assessment tool where users are asked to fill or select a set of questions. The questions are designed by using ISO/IEC 27001 [111] standard for basic security requirements are classified as categories.

The questionnaire-based method is also widely used in cyber insurance and insurers become more comfortable with estimating the premium when they have ample information on the security situation of an insured [91]. Not only, does the insurer receive the benefit, but the insured also understands its current security level and know what to improve. Our questionnaire-based risk assessment tool is also adapted for the cyber insurance model, in which we use the output as an input for the risk treatment tool.

2.2 Time-to-Compromise metric

One of the security level metrics is time-to-compromise, which is a required time for an organisation to be compromised by the attackers. From the attacker's standpoint, it is the expected time to successfully take down the system when gaining benefit is higher than the attacker's effort and cost. The approach has been studied by several researchers [17, 77, 74], i.e., Littlewood et al., [74] underlined that as time increases with a given

number of vulnerabilities and exploits, the probability of successful attack increases. This makes sense especially assuming the attackers' skill level and implemented security controls in the organisation.

Also, [17, 77] pointed out that defining the time-to-compromise provides us with a reasonable metric to measure the security level of organisations. In particular, the time-to-compromise metric has been proposed by A.Miles et al., (2006) [17] to reduce the security risk, which, the work was applied to a SCADA system as a real-case experiment. The work has been conducted with certain assumptions, i.e., the components of the system are visible to an attacker and the model does not address the dependency between vulnerabilities on different system components. Since there are attackers who possess different skill levels (from novice to advanced), the metric is considerably depending on their behaviour. D.John et al. (2009) [123] introduced an approach which incorporates the method of M.McQueen [17] into the attack tree approaches so that they can find the shortest path based on its required time. Similarly, W.Nzoukou et al., (2013) [19] proposed a framework for measuring the security of a network. The authors enhanced the idea presented by D.John et al. [123] by adding the CVSS (Common Vulnerability Scoring System).

In this work, we derived the idea of classic TTC metric by Mcqueen [17] and improved version by D.John et al., [123] to compute the probability of attack. The works are adapted into a competitive insurance model and improved for a multiple threats case.

2.3 Non-competitive Insurance Market

The competitive market model is most suitable for a theoretical investigation and often considered an impractical model. On the other hand, the non-competitive cyber insurance market is often found in today's so-

ciety. Insurers charge a higher premium to capitalise their safety against bankruptcy. Also, the insured's behaviour in the non-competitive insurance market model differs from the competitive insurance market model, where it has to pay an additional amount of fee, loading factor, for the premium [25, 37]. Furthermore, this additional fee can be served as an incentive to invest more so that the insured obtains a lower premium which is higher than one in a competitive market. Since the market is more practical, many researchers further conducted mathematical analyses in this market model. In particular, the change of security investments when cyber insurance available attracted more researchers.

Khalili et al., [108] investigated how interdependent risks are estimated in the premium by proposing the idea of including service providers (SPs). In this work, the authors found out that the insurers are profitable when they have security interdependence among the customers who are under one SP. They also found out that if they only provide the insurance for customers without insuring the SP (which will only participate as a third-party), the profit decreases comparing the previous scenario.

Ogut et al., [35] analysed the impact of security interdependency on this market, especially, investigated how security investments changes. The authors have concluded that the security investments decrease with the growth of the degree of interdependence and it rises when the immaturity of the market (loading factor) increases. They considered two main assumptions: 1) use only CARA (Constant Absolute Risk-Aversion) as a utility function, 2) the losses are taken too small with the comparison of insured's wealth. The latter assumption is particularly dangerous for insurance due to its adverse impact on the risk awareness behaviour of insureds. As opposed to this work, we propose a generic approach with the aforementioned assumptions (using CARA and CRRA (constant relative risk aversion) functions only as an example). More importantly, we

would like to show finding the optimal loading factor encourages the organisation/insured to invest up to the desired level. Also, there is not a study when the degree of interdependence is high. Therefore, we show how it affects the insured's behaviour on security investments when there is a cyber insurance option available.

Another interesting approach was conducted by P. Naghizadeh and M. Liu [29] for finding the optimal security investments. The model allows insurers to collect the proposals of all its insureds (the whole society) for the desired level of security investment and underlines the policies (i.e., premiums) correspondingly. The model is only acceptable under a condition where the participation of all insureds is obligatory. From the other side, our proposed solution enables voluntary participation and ensures that the insureds are still interested in buying the policy ($I \geq 0$) with a specified premium.

2.3.1 Effect of Security Interdependence in Competitive Market

As cyber insurance has gained much attention in the scientific literature [92, 25], researchers devoted their analyses to a unique factor, security interdependence, and its impact on cyber insurance [35, 49, 30, 38, 79]. This section will overview the most important papers and study how they reflected the idea.

External effect on self-protection has always been lying in cyber security field due to the interconnectedness, and it further affects the behaviour of an insured in cyber insurance. In particular, some researchers [35, 49, 30, 38] investigated its effect on relation between cyber insurance and security investments in self-protection.

H.Ogut et al., [35] provided a theoretical analysis of how a degree of security interdependence affects the insured's decision making when cyber insurance is available. The authors investigated its impact on different

market models – both competitive and non-competitive, as well as compared with an independent case. The analysis shows that the security investments fall with an increase of interdependency degree. Also, other researchers [50, 116], i.e., reached a similar conclusion. The results differ in a non-competitive insurance market, which shows that the insured is encouraged to invest when the market immaturity rises. H.Ogut et al. further investigated the impact of liability contagion and found that this enforcement can be an incentive to invest even more than a social optimum.

To keep both cyber insurance and security investments, others [27, 49, 38], i.e., Bolot et al., proposed a "fine and rebate" mechanism in which an insurer fines the insured that has not invested up to the desired level and rebates the one who does. The authors concluded that the mechanism only can be forced in a monopolistic/non-competitive market model without moral hazard. Pal et al., [38] also reached a similar conclusion that, without contract discrimination, cyber insurance cannot encourage the insured to invest. On the other hand, G. Schwartz, N. Shetty et al., [34, 43, 44] analysed the effect in the competitive insurance market model when there is a moral hazard. In their work, it is shown that cyber insurance cannot be an incentive to invest in self-protection.

Similar to the above-mentioned ones but a different variation of the "fines and rebates" mechanism was proposed by P.Naghizadeh et al., [31]. The main idea is a cooperation game between insureds and insurer who creates a society and suggests the optimum level of security to enforce. In this cooperation, each member of society recommends the optimal level which is eventually aggregated and rationally decided for enforcement by the insurer. Such a scheme can be an incentive without information asymmetry in place.

Overall, studies have shown different results depending on their assumptions. In this work, we would like to analyse the effect of security inter-

dependence in two cases; with and without cyber insurance. Comparing these cases will allow us to ensure whether a degree of security interdependence encourages the insured to invest or not in a competitive insurance market.

Chapter 3

Optimisation of cyber insurance coverage with selection of cost effective security controls.

3.1 Introduction

We first start analysing the relation of cyber insurance and security investments in a competitive insurance market which is often conceptualised by researchers due to its simplicity and formality [25]. Moreover, the premium[1] is actuarially estimated based on a risk assessment process, and it is often referred to as a fair estimation [25]. This indicates that the risk assessment process is the first challenging step in cyber insurance and it should be as accurate as possible.

Most papers on cyber insurance, i.e., [35, 37], assume a single threat, which simplifies the model in the theoretical-oriented analysis. On the other hand, in practice, organisations face various types of threats during a certain period. This practical case makes the current models abstract since there are different losses triggered by those identified threats (e.g., see examples of threats from the ISO/IEC 27005 standard [98]). More-

[1] fee from the insured to the insurer for potential loss cover

over, the current cyber insurance approaches assume that the probability of an attack or the threat frequency is computed by knowing the level of security investments [25]. It is contradicted in a real-world case where the experts should devise a method to tell what security controls are the best to meet the highest level of security protection. In this thesis work, we refer to the security controls as those which are used to mitigate the cyber risks in both proactive and reactive manners. For example, it could be a firewall or access control policy as administrative control. Also, taking into consideration that some controls are already installed in prior, which makes the further selection of security controls more complex (i.e., some amount of investments could be already spent and its current distribution could be not cost-efficient). In particular, some legal requirements or contractual obligations could force the organisation to install, in some cases, expensive but not efficient enough controls. In this case, it is not enough to consider only the amount of investments, but it is required to determine the best additional improvement of security having in mind existing (probably, not cost-efficient) security configuration. To that end, our first concern is to provide a solution for the following problem: " *When the market is competitive and there are multiple-threats expected to occur, what is the best approach to minimise the overall risks by distributing the security expenditure among cyber insurance and security investments options?*".

To treat those identified and assessed risks, the best security control selection is the core challenge in both risk mitigation and transfer options, and it has received a lot of attention from various researchers. The problem is often seen as a classic 0-1 Knapsack Problem [53] based on the cost of security controls and their capability of reducing the damage of threats (effectiveness of control). Several authors [54, 55, 56, 57] derived and improved the core idea of the classic 0-1 Knapsack Problem to optimise the security control selection process. However, existing Knapsack Problems

have several limitations, i.e., it uses the security budget as a limit to find the controls (even if some controls are not efficient). Thus the approach is not cost-effective in some cases.

Furthermore, the utility functions become computationally ineffective (i.e., existing pseudo-polynomial solutions like Dynamic Programming (DP) cannot be applied) because of the usage of risks. It could be applicable in some specific cases where, for instance, only one threat is considered [2, 102]. On the other hand, when the problem becomes more complex, i.e., multiple-threats in our case, it will require more conceptually robust approaches. Therefore, other approximate solutions like Evolutionary Algorithms (i.e., Genetic Algorithms (GA)) and Greedy approaches were introduced. These solutions are much faster and less resource-consuming in comparison with pseudo-polynomial ones. However, a drawback of these approaches is to finding the nearest-optimal answers in complex scenarios instead of the optimal ones. Thus, we look for an applicable solution in the sense of Simon [105]. Particularly, we derive and improve both exact and approximate algorithms in harmony with a theoretical investigation considering the multiple-threats in the competitive insurance market model.

The chapter is structured as follows. Section 3.2 discusses the existing problems in a competitive insurance market and formalise them mathematically. Section 3.3 introduces our proposed solutions for those identified issues. We validate our work in Section 3.4 with implementing the solution for different use cases. Also, we discuss the limitations taken in this work and further directions in Section 3.5. Finally, Section 3.6 summarise the chapter by shedding the brief insight.

3.2 Problem specification

This section casts the cyber insurance and security investment problem in a competitive insurance market model with a consideration of the multiple-threats case. In particular, we decompose the specific problem of mapping security controls with the cyber insurance premium. We analyse the problems systematically, starting from the baseline scenario where no cyber insurance option is available to the case of having both cyber insurance and security controls to treat the risks.

3.2.1 Single threat case without insurance

Before we introduce the main problem, we begin with a basic scenario in which an organisation invests x amount of investments to mitigate the identified risks for a certain period of time. Since it is highlighted that organisation always faces a residual risk even though it installs security controls. If we assume a threat passes through a set of controls, it causes certain losses denoted as L. We assign W^0 for the initial wealth of the organisation and W for the final wealth after a certain period (usually a year). Taking into account of above-mentioned factors, we can compute the final wealth given as:

$$W = W^0 - L - x \tag{3.1}$$

It is intuitively understandable that without any threats, $L = 0$, and otherwise, the organisation will face some $L > 0$. Naturally, the organisation always aims for a maximum of W by optimising the security investments x. The following equations represent our two scenarios:

$$\begin{aligned} W_{NN} &= W^0 - x \qquad with\ no\ threats \\ W_{NL} &= W^0 - x - L, \qquad with\ \ threats \end{aligned} \tag{3.2}$$

where W_{NN} and W_{NL} represent the final wealth in no insurance case without and with threats, respectively. Now, we are interested in defining the probability of successful events occurring p, which causes the loss. The probability of successful attacks further depends on the number of investments for the self-protection ($p(x)$). Thus, our expected wealth (E(W)) is given as:

$$E(W) = p(x)(W^0 - x - L) + (1 - p(x))(W^0 - x) \tag{3.3}$$

So far, several works [25] investigated the problem of security investments optimisation. However, no work cast the problem of having multiple-threats, particularly in cyber insurance concept. In the following sub-sections, we analyse the main problems in-depth.

3.2.2 Multiple-threats case without insurance

In practice, we face different sorts of threats, where each of them has the potential to cause different losses. Let us consider an organisation which has identified n_t ($n_t \in \mathbb{N}^+$) relevant threats. For each threat, a corresponding expected loss has been defined $\vec{L} = \langle L^1, L^2, ..., L^{n_t} \rangle$, where $\vec{L}$ is a vector and $L^i (1 \leq i \leq n_t)$ is its i^{th} member. Now it is perspicuous that the organisation invests in self-protection by taking into account all identified threats. Basically, these investments will be spent on a set of security controls K_s to mitigate the risks, and this set can be seen as a subset of all available security controls K (e.g., the ones that could be found in ISO27002 [75] or NIST 800-53 [9]). If we assume the cost of control to be a function, its result will be a finite non-negative value $c : K \mapsto \mathbb{N}^+$ (i.e., thousands of Euro). Once we know the cost of each control, the overall cost of $K_s \subseteq K$ ($c(K_s)$) is computed as

$$c(K_s) = \sum_{\forall k \in K_s} c(k). \tag{3.4}$$

The probability of a successful attack which we used so far will be also a vector for n_t threats, $\vec{p}(K_s) = \langle p^1(K_s),\ p^2(K_s), ...,\ p^{n_t}(K_s)\rangle$. Now, if we know the frequency of threats occurrences $\vec{F} = \langle F^1, F^2, ..., F^{n_t}\rangle$, the overall risk for the organisation can be found as follows.

$$Risk(K_s, x, \vec{L}) = (\vec{F} \odot \vec{p}(K_s)) \times \vec{L}, \tag{3.5}$$

where $\vec{a} \times \vec{b}$ is a usual matrix multiplication of two vectors given as $\vec{a} \times \vec{b} = \sum_{i=1}^{n_t} a^i \cdot b^i$ and the Hadamard product of two vectors $\vec{a}$ and $\vec{b}$ is a vector $\vec{c} = \vec{a} \odot \vec{b} = \langle a^1 \cdot b^1, a^2 \cdot b^2, ..., a^{n_t} \cdot b^{n_t}\rangle$. We further define $\vec{z} = \langle z^1, z^2, ..., z^{n_t}\rangle$ as a random vector of numbers for threat occurrences (one per threat) and $p(\vec{z}|K_s)$ be the probability that the considered organisation will face $\vec{z}$ incidents for some period of time conditional on the implemented controls K_s. Now our final wealth after occurrence of $\vec{z}$ threats can be defined as:

$$W(\vec{z}, K_s, x) = W^0 - x - \vec{z} \times \vec{L} \tag{3.6}$$

The goal of the organisation is to maximise its expected wealth, i.e.,

$$E[W(\vec{z}, K_s, x)] = \sum_{\forall \vec{z}} (W^0 - x - \vec{z} \times \vec{L}) \cdot p(\vec{z}|K_s) = W^0 - x - \sum_{\forall \vec{z}} (\vec{z} \cdot p(\vec{z}|K_s) \times \vec{L} \tag{3.7}$$

We note that $\sum_{\forall z} (\vec{z} \cdot p(\vec{z}|K_s)^2$ is the mean number of occurrences, previously defined as $\vec{F} \odot \vec{p}(K_s)$. Finally, our optimisation problem can be seen

[2] "$\cdot$" is the scalar multiplication defined as $\vec{a} \cdot b = \langle a^1 \cdot b, a^2 \cdot b, ..., a^{n_t} \cdot b\rangle$

as

$$\max_{x,K_s} E[W(\vec{z}, K_s, x)] =$$
$$\max_{x,K_s}[W^0 - x - (\vec{F} \odot \vec{p}(K_s)) \times \vec{L}] =$$
$$\max_{x,K_s}[W^0 - x - Risk(K_s, x, \vec{L})] \tag{3.8}$$

or

$$\min_{x,K_s}[x + (\vec{F} \odot \vec{p}(K_s)) \times \vec{L}] \tag{3.9}$$

3.2.3 Multiple-threats in Insurance case

Until this point, we have only considered a risk mitigation technique to deal with identified risks. However, depending exclusively on security controls is not enough to reduce the risks, and to that end, we have another option, cyber insurance. If an organisation decides to have a cyber insurance option, it is offered to pay a premium P and expects some coverage (called indemnity $\vec{I}$) if an incident were to occur. Since our loss is a vector, the indemnity is also considered as a vector of size n_t. In cyber insurance, the indemnity is always equal or lower than loss, i.e., $\forall i,\ I_i \leq L_i$, and the premium is computed through an estimated risk. In other words, we can simply assume the following equation to compute the premium in a competitive insurance market [25]:

$$P = Risk(K_s, x, \vec{I}) \tag{3.10}$$

Now, after occurrence of $\vec{z}$ threats (i.e., similar to Equation 3.7), our final wealth is given as:

$$W(\vec{z}, K_s, x, \vec{I}) = W^0 - (\vec{F} \odot \vec{p}(K_s)) \times \vec{I} - x - \vec{z} \times (\vec{L} - \vec{I}), \tag{3.11}$$
$$where\ \vec{I} - \vec{L} = \langle I^1 - L^1, I^2 - L^2, ..., I^{n_t} - L^{n_t} \rangle.$$

Similar to other economic models [25, 35, 41], the organisation is preferred to be risk-averse and uses utility of possessing a certain amount of wealth $U(W)$ instead of the pure wealth W itself. In that case, the utility function is considered to be continuous, non-decreasing, and concave, i.e., $U'(W) > 0$ and $U''(W) < 0$.

$$U(W(\vec{z}, K_s, x, \vec{I})) = U(W^0 - (\vec{F} \odot \vec{p}(K_s)) \times \vec{I} - x - \vec{z} \times (\vec{L} - \vec{I})). \quad (3.12)$$

Finally, the expected utility is equal to:

$$E[U] = \sum_{\forall \vec{z}} p(\vec{z}|K_s) \cdot U(W^0 - (\vec{F} \odot \vec{p}(K_s)) \times \vec{I} - x + \vec{z} \times (\vec{I} - \vec{L})). \quad (3.13)$$

Thus, our goal is to maximise the expected utility ($E[U]$) by finding the optimal x, $\vec{I}$ and K_s.

3.3 Competitive Insurance Market Analysis

The first and core part of the thesis is to devote our solution to the distribution of cyber security expenditure on cyber insurance premium and security investment (i.e., installation of security controls) in a competitive insurance market. In particular, the problem arises when there are multiple threats expected to occur. As we defined in the problem section, there are no current models to find the optimal investment and indemnity when there are multiple threats available. The first step is to find the indemnity as is mathematically shown in the following sub-section.

3.3.1 Indemnity

Even though it has already been proven in the literature that, for a competitive insurance market, the optimal indemnity is equal to loss [25], we

would like to find out whether this condition also meets in a multi-threats scenario. In this regard, we apply Jensen's inequality for a concave function (for any concave function $\phi(t)$ $E[\phi(t)] \leq \phi(E[t])$) for Equation 3.13:

$$\sum_{\forall \vec{z}} p(\vec{z}|K_s, x) \cdot U(W^0 - (\vec{F} \odot \vec{p}(K_s|x)) \times \vec{I} - x + \vec{z} \times (\vec{I} - \vec{L})) \leq$$
$$U(\sum_{\forall \vec{z}} p(\vec{z}|K_s, x) \cdot \Big[W^0 - (\vec{F} \odot \vec{p}(K_s|x)) \times \vec{I} - x + \vec{z} \times (\vec{I} - \vec{L})\Big]) =$$
$$U(\left[\sum_{\forall \vec{z}} p(\vec{z}|K_s, x)\right](W^0 - x) - \left[\sum_{\forall \vec{z}} p(\vec{z}|K_s, x)\right] \cdot \Big[(\vec{F} \odot \vec{p}(K_s|x)) \times \vec{I}\Big] +$$
$$\left[\sum_{\forall \vec{z}} p(\vec{z}|K_s, x) \cdot \vec{z}\right] \times \vec{I} - \left[\sum_{\forall \vec{z}} p(\vec{z}|K_s, x) \cdot \vec{z}\right] \times \vec{L}).$$

Since $\sum_{\forall \vec{z}} p(\vec{z}|K_s, x) = 1$ and $\vec{F} \odot \vec{p}(K_s|x) = \sum_{\forall \vec{z}} p(\vec{z}|K_s, x) \cdot \vec{z}$, we get:

$$U(W^0 - x - \Big[(\vec{F} \odot \vec{p}(K_s|x)) \times \vec{I}\Big] + (\vec{F} \odot \vec{p}(K_s|x)) \times \vec{I} - (\vec{F} \odot \vec{p}(K_s|x)) \times \vec{L}) =$$
$$U(W^0 - x - (\vec{F} \odot \vec{p}(K_s|x)) \times \vec{L}).$$

The last part ($U(W^0 - x - (\vec{F} \odot \vec{p}(K_s|x)) \times \vec{L})$) is the expected utility if $\vec{I} = \vec{L}$. In other words, Equation 3.13 is maximal if $\vec{I} = \vec{L}$.

It indicates that we can reduce Equation 3.13 for a risk averse organisation given as:

$$\max_{x, K_s} U(W^0 - x - (\vec{F} \odot \vec{p}(K_s)) \times \vec{L}). \tag{3.14}$$

Since our utility function is non-decreasing, we can simply minimise the following part (called *expenditure*) to maximise the utility:

$$\min_{x, K_s}(x + (\vec{F} \odot \vec{p}(K_s)) \times \vec{L}). \tag{3.15}$$

Our problem further can be seen similar to what defined in Section 3.2.2 without an insurance case. In this case, the premium is considered as the accepted risk so that the organisation simply minimise the sum of

residual risk and security investments for self-protection. Thus, our further contribution could be applied if one of the conditions (in Equation 3.9) described above is found to be applicable.

3.3.2 Selection of security controls

Finally, the main problem is to know how to compute $p(K_s|x)$ and devise the best approach for selecting K_s so that we will be capable of minimising the Equation 3.15. This has to be done under the circumstances of equal or fewer investments than x.

Let us denote $\pi^j(k) \in [0;1]$ as the probability of survival that, only if a threat j passes through the installed control $k \in K_s$. On the given condition of the value of $\pi^j(k)$ to be equal to either 0 or 1, we may say that the control k protects the assets against the threat j or it is impractical to place in, respectively. Same as the probability of attack that we defined, the probability of survival is also a vector, $\vec{\pi}(k)$ if k is installed, and the overall probability of survival can be computed as[3]:

$$\vec{\pi}(K_s) = \prod_{\forall k \in K_s} \vec{\pi}(k), \tag{3.16}$$

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

Now, we are able to connect $\vec{\pi}(K_s)$ and $\vec{p}(K_s|x)$. We say that $\vec{p}(K_s|x) = \vec{\pi}(K_s)$ if K_s minimises Equation 3.15 and its overall cost is below z:

$$\min_{\forall K_s \subset K} (\vec{F} \odot \left[\prod_{\forall k \in K_s} \vec{\pi}(k) \right]) \times \vec{L} + x \quad and \quad \sum_{\forall k \in K_s} c(k) \leq x. \tag{3.17}$$

Now, Equation 3.17 becomes the main problem to solve in the following section.

[3]We assume the effect of security controls independent from each other.

3.3.3 Algorithmic Solutions

The problem, Equation 3.17, brings the idea of applying the classic 0-1 Knapsack Problem (KP). However, we derive the main notion instead of an entire concept of the legacy KP. Instead of summing the values, the idea is to multiply for aggregation of items (i.e., security controls) and has a complex utility function (multiplications and summations). Moreover, we aim for the minimal whereas the original KP is conceptualised for the maximisation. It is also worth mentioning that the utility function does not order the preservation of countermeasures, meaning that if we add the same countermeasure to one set that was riskier than another one, the resulting set may become less risky. Furthermore, the budget limit is another criterion in KP and we look for finding the optimal budget rather than assuming it as a criterion to select the controls. In other words, even though the problem looks familiar with the original KP, there are several modifications to find the cost-efficient distribution of the expenditure.

Since we consider multiple-threats, the problem can be seen as the 0-1 multi-objective KP, i.e., a 0-1 KP with many utilities to maximise (i.e., threats to reduce, in our case). For this problem, there are several optimisation solutions [68, 103]. The solution does not provide a single algorithm, but we will propose several methods with the improvements and compare them for different scenarios. The algorithmic solutions will be as follows:

- find the exact solution by implementing Dynamic Programming,
- improve the Dynamic Programming solution (e.g., embedding the Projection idea),
- adapt a couple of approximate solutions (e.g., Greedy and Genetic Algorithms) to the problem
- conduct an analysis for the applicability of the solutions (will be ad-

dressed in Results chapter).

Dynamic Programming We start with the Dynamic Programming (DP) solution to solve the 0-1 multi-objective KP by adapting the main concept of the work by Bazgan et al., [68]. In both theory and practice, the DP is applied if the whole problem could be seen as recursively nested sub-problems. In particular, DP solves the optimisation problem by breaking the whole problem down into simpler sub-problems and finds the optimal solution through a series of iterations and comparisons.

Let all the elements of K as $j = 0, 1, ..., n_K$ (where n_K is the size of K) and check all countermeasures to know whether it satisfies the requirement or not in order to select or reject, respectively. Basically, we will check all controls $j = 0, ..., q$ and continue with $j = q + 1, ..., n_k$, once we reach a control k_q

To represent the value, we denote the positive integer values as costs of countermeasures, such that $\forall k \in K$ $(c(j) = C \cdot m_j)$, where C is the greatest common divisor for all costs and m_j is just some positive natural value $\forall j, m_j \in \mathbb{N}^+$. In this case, the common divisor C will be the increasing step to limit the computations in every cell (i.e., $x = C \cdot m$, where $m = 0, 1, ..., m_{max}$). To align the costs of countermeasures and budget limit, we need an auxiliary matrix T.

To advance in two directions (i.e., considered controls and budget limit) we need an auxiliary matrix T. In this regard, every cell $T[j][m]$ keeps the best solution considering the first j controls and budget limit $x = m \cdot C$ (the probability is computed with Equation 3.16). Based on this idea, the whole process checks all controls as it keeps increasing the budget with the common divisor. In other words, we are looking for the value (and associated selection of controls) of the cell $T[n_t][m^*]$, and this will be the optimal solution for the whole problem, while every $T[j][m]$ (for $j < n_t$

and $m < m^*$) are the sub-problems.

Since we consider multi-threats, the combination of different security controls can be provided within the budget limit, where every cell can keep several alternatives. In the traditional method for solving 0-1 KP, every sub-problem (i.e., a selection of alternatives for $T[j][m]$ $j < n_t$ and $m < m^*$) could be solved, because the utility function used is order-preserving. Working with a multi-objective optimisation problem, we have no definitive criteria to select the best solution for a sub-problem apart from classifying them as *dominated* and *non-dominated* vectors. Naturally, to simplify the computation, all dominated vectors can be removed.

Basically, the core of the algorithm for 0-1 multi-objective KP could be seen as the following recursive algorithm:

1. $T[0][m] = 1$;
2. if $c(k_j) > m \cdot C$ (the new item is more expensive than the current cost limit);
   - Then:
     $T[j][m] = T[j-1][m]$
   - Else:
     $T_{add} = \bigcup_{\forall \vec{t} \in T[j-1][m-c(k_j)/C]} \vec{t} \odot \vec{\pi}(k_j)$
     $T[j][m] = non - dominated(T[j-1][m] \cup T_{add})$

Figure 3.1: Recursive algorithm

As opposed to traditional methods, we consider the security budget limit as not a given value but this value will be found (optimized x^*) by solving Equation 3.15. Also, the recursive algorithm does not require the security investment to be bound and this allows us to start the investments from 0 to the optimal one (also extending matrix T for new x to check). by increasing it. At the same time, we should ensure the minimum number of iterations to save both time and resource.

We can re-write Equation 3.15 as follows, denoting the optimal premium

(or risk) if x amount is invested in self-protection as $P^*(x)$:

$$\min_{\forall x}(P^*(x) + x). \tag{3.18}$$

Considering 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 y:

$$x_r + P^*(x_r) > x_{r+y} + P^*(x_{r+y}); \tag{3.19}$$

$$x_{r+y} < P^*(x_r) + x_r - P^*_{min}; \tag{3.20}$$

$$, where\ P^*_{min} = \vec{F} \odot \left[\prod_{\forall k \in K} \vec{\pi}(k)\right]) \times \vec{L}. \tag{3.21}$$

The aforementioned two equations (15 and 16) lead us to the following observations. First, Equation 3.19, shows how the selection of optimal value is found by comparing the current best value (i.e., up to step r) with the next ones ($y > 0$). The latter, Equation 3.20, limits the iteration since there will be no more efficient solutions. We also may find the first limit, which is: $x_0^{limit} = P^*(0) - P^*_{min}$, assuming that P^*_{min} is the minimal possible premium/risk that is computed with all available countermeasures $K_i = K$ installed. On the hand, if the organisation sets a security investment limit x^{lim} and $P^*(x_r) + x_r - P^*_{min} > x^{lim}$ initially, we should link the further steps with $x_{r+y} < x^{lim}$. To that end, the solution will not be greater than the budget but could be lower than the budget. We also reset the limit for each better x, 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 $r + y - 1$ steps) and x_{r+y} be even better than x_r, i.e.,:

$$P^*(x_r) + x_r > P^*(x_{r+y}) + x_{r+y}. \tag{3.22}$$

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

$$P^*(x_r) + x_r - P^*_{min} = x_r^{limit}\ ;\quad P^*(x_{r+y}) + x_{r+y} - P^*_{min} = x_{r+y}^{limit}. \tag{3.23}$$

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

Dynamic Programming Based on the described theory based idea, we now introduce the algorithmic solution (Algorithm 1), which a) finds the optimal investments in self-protection x^*; b) ensures the lowest expenditure $((\vec{F} \odot \vec{pr}(K_s^*|x^*)) \times \vec{L} + x^*)$. Even though the core of the dynamic programming approach for 0-1 multi-objective KP [68] has been re-used, the adaptation and modification allow us to take the optimal investments as an output rather than taking it as an input. The algorithm starts defining the initial variables and functions for the input i.e., cost function and single loss expectancy, line 3 and 6 respectively. Another important contribution in this algorithm is that it allows the organisation has already invested some amount x_{init} in its self-protection (installing an initial set of controls K_{init} which yields the initial probability of attack $\vec{p}_{init}$) due to the basic mandatory regulations i.e., GDPR. Yet, for further analysis, the initial set of controls are not going to make an impact since the goal is to select the best ones among the available controls: $K_{init} \cap K = \emptyset$.

Before start checking the controls, the algorithm computes minimal premium P_{min} and sets up initial values (9 and 16). Since finding the GCD is well-known and, thus, is not going to be described in details and we just define the function as $GCD(\cup_{\forall k \in K} c(k))$.
As it is stated in Equation 3.20, the limit x is increased with its counter m until $exp - P_{min}$ condition does not hold (line 17). In more details, the computation considers all controls one by one (line 19) for every increased limit x. And for each control, we compare: 1) a set of previously selected controls with k_j $(\bigcup_{\forall l} \vec{\pi}(k_j) \odot T[j-1][m - c(k_j)/C][l])$, 2) and the best selection of controls without k_j $(T[j-1][m])$ (line 21). In every cell, there are only non-dominated elements left to be considered for the further computation.

If the cost of next control is higher than the investment x, we keep the previously selected controls and the corresponding probability of survival

Algorithm 1: Selecting the best set of countermeasures

Function(*searchForOptimalInvesments*)
Input: K, c, π, $\vec{F}$, $\vec{L}$, x_{init}, p_{init}, C
Require:
K // a set of countermeasures
$c : K \mapsto \mathbb{N}$ // cost function
$\pi : K \mapsto 2^{[0;1]}$ // survival probability per threat function
$\vec{F}$ // frequency vector of $\mathbb{R}^+$ values
$\vec{L}$ // single loss expectency vector of $\mathbb{N}^+$ values
$x_{init} \in \mathbb{N}$ // initial investments
$\vec{p}_{init}$ // initial overall probability of survival vector of values from $[0; 1]$
Ensure: lowest $(\vec{F} \odot \vec{pr}(K_s|x)) \times \vec{L} + x$ for optimal security investment x^*
$exp := (\vec{F} \odot \vec{p}_{init}) \times \vec{L} + x_{init}$
// Remember the initial expenditure as optimal
$P^*_{min} := \vec{F} \odot [\prod_{\forall k \in K} \vec{\pi}(k)]) \times \vec{L}$
$x^* := x_{init}$ // Optimal Investment starts with x_{init}
$\forall q \; T[q][0] := \{\vec{p}_{init}\}$ // a dynamic matrix of optimal probabilities. Add new (and the first) column $x = x_{init}$, with one vector $\vec{p}_{init}$
$C := GCD(\cup_{\forall k \in K} c(k))$ // the greatest common divisor for cost of controls
$x := C$ // first increase of investments
$m := 1$ // investment counter starts with 1
$n_k := |K|$ // the size of set K
while $x + x_{init} \leq exp - P^*_{min}$ **do**
// Do while x is below the optimal expenditure
  $\forall j \; T[j][m] := \{\vec{p}_{init}\}$ // new column is set with vector $\vec{p}_{init}$
  for $j := 1, n_k$ **do**
  // for all countermeasures
    if $(c(k_j) \leq x \;)$ **then**
    // check the cost limit
      $T[j][m] := non - dominant \begin{cases} \bigcup\limits_{\forall l} \vec{\pi}(k_j) \odot T[j-1][m - c(k_j)/C][l] \\ T[j-1][m] \end{cases}$
      // store all non-dominant vectors comparing two sets: with new control and without.
    else
      $T[j][m] := T[j-1][m]$
      // continue without adding new control j
  for $l := 0, |T[n_k][m]|$ **do**
  // for all vectors stored in $T[n_k][m]$
    if $(\vec{F} \odot T[n_k][m][l]) \times \vec{L} + x + x_{init} < exp$ **then**
    // reduced the expenditure?
      $exp := \vec{F} \odot T[n_k][m][l]) \times \vec{L} + x + x_{init}$ // Store this expenditure as optimal
      $x^* := x$ // Remember these investments as optimal
  $x := x + C$
  $m := m + 1$
Return: exp, x^*

$T[j-1][m]$ (line 23). As we mentioned above, the computation is not done as it has been introduced originally (sum and aim for the maximal), instead, it multiplies the values when there is an additional control added to the set.

The important part is to compare the current computed security investment x with the previous one after considering all controls Equation 3.19. If it is lower than the preceding investments with some vectors from $T[n_k][m]$, we reset the optimal security investments as the new one (line 27). More importantly, in line 26, we also replace the expenditure with the new one for the further computations (according to the condition in Equation 3.20).

In line 17, we find the optimal security investment and the lowest security expenditure until the condition does not meet. Also, we have developed a simple backward algorithm to find out which controls are selected (Algorithm 2). The algorithm simply reverses the selection process in a simplified way and remembers the selected control in a list.

Algorithm 2: Recover selected controls

```
1  Function(BackTrack)
   Input: x*, c, T, C
   Require:
2  x*          // optimal investment found by searchForOptimalInvestments algorithm
3  c                                                          // cost of controls
4  T              // auxiliary matrix T from searchForOptimalInvestments algorithm
5  C                                                      // CGD for control cost
   Ensure: Optimal K_s
6  K_s := ∅
7  x := x*                                  // we start with optimal investment level
8  for i := 0 to n do
       // Iteration starts from the end of control's list
9      if x − c[n − i − 1] < 0 then
10         if T[n − we − 1][x/C] ≠ T[n − i][x/C] then
11             K_s.append(k[n - i])        // add n − i -th control the selected controls list
12             x := x - c[n -we - 1]        // Decrease the optimal investment by the cost of
                (n-i-1)-th control
   Return: K_s
```

[**Dominance criteria**] **Dynamic Programming** In algorithm (1), we have used the Pareto optimality, i.e., we checked that every element of one vector is better or equal (in our case, lower or equal) than the corresponding one from another vector. However, when the number of security controls increases, the non-dominated vectors for every cell rapidly grows, and this process significantly slows the algorithm. For this reason, we have studied possible ways to improve the algorithm.

We have found two viable methods, i) Projection and ii) Sorting to foster the algorithm. The projection idea aims to strengthen the dominance criteria, by looking to the remaining controls and assuming the worst case for a vector with lower risk. If the vector under these conditions still results in a lower risk than its opponent, we discard the second vector. Sorting security controls by their cost, leaving the expensive ones for later consideration, serves to reduce the number of potential alternatives (and non-dominated vectors) at the end.

To apply the projection method, we first compute the best case scenarios for all controls with the multiplication of values for threats starting from the latest control. To store these values, we create a table $Best[n_k][i]$:

$$Best[j][i] = \prod_{q=n_K-1}^{j} \pi(k_q)[i] \tag{3.24}$$

So far, we know the lowest probability of survival for every set of considered controls (e.g., by j-th one) if all remaining controls will be installed. Now, we compare the two vectors $\vec{p}$ and $\vec{p'}$ after considering only j-th control and check if the risk for the first one is lower than for the second one, i.e.

$$\vec{F} \odot (\vec{p} - \vec{p'})) \times \vec{L} < 0. \tag{3.25}$$

Let's assume O be set of all indexes for threats ($|O| = n_t$) and for some $i \in \hat{O} \subset O$ $p[i] > p'[i]$ and for others $i \in O \backslash \hat{O}$ $p[i] \leq p'[i]$. We form a vector

$\vec{D}$ with n_K values, as follows:

$$D[i] = \begin{cases} Best[j][i] & if\ i \in \hat{O} \\ 1 & if\ i \in O \backslash \hat{O} \end{cases} \tag{3.26}$$

Then, we check if the first vector still produces the lower risk when we reduce the survival probability for threats from $\hat{O}$.

$$\vec{F} \odot (\vec{D} \odot (\vec{p} - \vec{p'}))) \times \vec{L} < 0. \tag{3.27}$$

If this case becomes "True", we can simply remove the second vector from the following computations because having the first set will always result in a lower risk for all possible scenarios for the future. Note that this definition of dominance includes the former Pareto optimal approach in Algorithm 3.

[**Theoretical part**] **Greedy** We have introduced only DP-based solutions which are accurate for finding the answer and perfectly fine with small input. However, when we have a large and complex input, the algorithms appear to be struggling to complete the computation in a preferable time and require more recourse. Therefore, we look for some approximate solutions which work faster but often find nearly optimal answers.

One of the well-known approaches is a Greedy solution [76], which significantly saves time and recourse. The reason for these advantages is that it adds (or remove) the elements which separately contribute the most (or the least) to the overall goal. Even though it is simple to implement and has some pros, the approaches do not always provide the optimal solution but the nearest ones.

[**Algorithm**] **Greedy** The approach that we develop is to select all controls in the beginning and remove the controls one by one at the same time

Algorithm 3: Projection Function of the DP

```
1  Function(newDominanceCheck)          // Checking new dominance using projection idea
   Input: VectorsA, VectorsB, Best[j], F⃗, L⃗, n_t
   Require:
2  VectorsA, VectorsB                   // two sets of vectors to check for dominance
3  Best[j]                              // A vector with corrective values for the current step j
4  F⃗                                    // frequency vector of ℝ⁺ values
5  L⃗                                    // single loss expectency vector of ℕ⁺ values
6  n_t                                  // number of threats
   Ensure: A set of non-dominated vectors
7  for q < |VectorsA| do
8      for l < |VectorsB| do
9          v1 := 0                      // vector q is dominating
10         v2 := 0                      // vector l is dominating
11         for k < n_t do
12             if (VectorsA[q][i] − VectorsB[l][i]) < 0 then
13                 v2 := v2 + (VectorsA[q][i] − VectorsB[l][i]) · F[k] · L[i]
14                 v1 := v1 + (VectorsA[q][i] − VectorsB[l][i]) · Best[j][i] · F[k] · L[i]
15             else
16                 v2 := v2 + (VectorsA[q][i] − VectorsB[l][i]) · Best[j][i] · F[k] · L[i]
17                 v1 := v1 + (VectorsA[q][i] − VectorsB[l][i]) · F[k] · L[i]
                                        // new vector is dominating
18         if v2 > 0 then
19             remove vector q from VectorsA
                                        // old vector is dominating or the same
20         if v1 <= 0 then
21             remove vector l from VectorsB
22 result := VectorsA ∪ VectorsB
```

comparing which control's removal reduces the overall expenditure more than the removal of others. This process is iterated until we are not able to remove any controls without decreasing the expenditure. The main functions (4, 5, 6) of the algorithm are presented as follows.

The core function, *OptimalSelection*, is shown from line 1 to 12 in algorithm 4. The algorithm assumes that initially all controls are selected and gradually remove the ones whose absence reduces the overall expenditure more than other controls. The iteration continues until no security control reduces the total expenditure. The overall expenditure is computed in an

Algorithm 4: The main function for Greedy approach

```
1  Function(GreedySelection)
   Input: c, π, L⃗, p⃗_init, F⃗
   Ensure: lowest minCost and optimalBudget for optimal security investment x*
2  minCost, optimalBudget := Calc(c, π, L⃗, p⃗_init, F⃗)   // call Calc function to minCost and
     optimalBudget
3  index := FindWorstControl(c, π, L⃗, p⃗_init, F⃗)
4  while index ≠ -1 do
       // iterate until the loop ends
5      delete c[index]                                  // Delete the cost of the worst control
6      delete π[index]        // Delete all probabilities of survival related to the worst
         control
7      currentCost, currentBudget := Calc(c, π, L⃗, p⃗_init, F⃗)   // call Calc function to
         currentCost and currentBudget
8      if currentCost < minCost then
           // check the condition and replace the minCost with currentCost if it
             meets
9          minCost := currentCost
10         optimalBudget := currentBudget
11     index := FindWorstControl(c, π, L⃗, p⃗_init, F⃗)
12 return minCost, optimalBudget
```

Auxiliary Function *Calc* (Algorithm 5) with a set of currently selected controls; and the function *FindWorstControl* (Algorithm 6) selects the worst control to be removed.

Algorithm 5: Calculation function of Greedy approach

```
1  Function(Calc)                  // This function computes the minCost (expenditure)
   Input: c, π, L⃗, p⃗_init, F⃗
2  minCost := 0
3  for i := 1 to length(L⃗) do
4      prob := 1                                        // expected loss per threat i
5      for j := 1 to length(c) do
6          prob := prob · π[j][i]
7      minCost := F⃗[i] · L⃗[i] · p⃗_init[i] · prob   // put the sum of expected losses to the minCost
8  optimalBudget := sum(c)                            // put sum of costs to opimalBudget
9  minCost := minCost + optimalBudget                 // computes the overall expenditure
10 return minCost, optimalBudget
```

Algorithm 6: Removal of the worst control for Greedy approach

```
1  Function(FindWorstControl)                          // function for finding worst controls
   Input: c, π, L⃗, p⃗_init, F⃗
   Ensure: Index of a control with the smallest risk reduction
2  n := length(c)                                      // define the length of costs
3  if n == 1 then
4      return −1
5  h := length(L⃗)                                     // define the length of probability of survival
6  s := sum(c)                                         // define the length of overall cost
7  minCost, temp := Calc(c, π, L⃗, p⃗_init, F⃗)          // call the Calc() function
8  index := -1
9  for j := 1 to n do
10     val := 0                                        // the residual risk without j-th control
11     for i := 1 to h do
12         prob := 1                                   // probability of survival of threat i
13         for l := 1 to n do
14             if l ≠ j then
15                 prob := prob · π[j][i]              // add the relation of π
16             val := val + F⃗[i] · L⃗[i] · p⃗_init[i] · prob
17     currentCost := val + s - c[i]                   // compute the currentCost
18     if currentCost < minCost then
19         minCost := currentCost                      // update the minCost
20         index :=we                                  // take the i-th control's index and return
21 return index
```

GA Another frequently adapted optimisation solution is the Genetic Algorithm (GA) [103, 101], one of the Evolutionary Algorithms, and it provides the optimal or nearest optimal solutions in a short time. We derived the main idea of GA which [103, 101] proposed, however, to fit into our problem, we have made some modifications and improvements. The first problem was to deal with the initial population creation. If we initialise the population entirely random, the computation and selecting processes consume an enormous time to satisfy the fitting criteria (i.e., see the Equation 3.15). To solve this issue, we have applied the semi-random method for the initial population. The idea (see algorithm 8) is to convert some percentage of genes[4] in the generated chromosome into 1. Then it checks whether

[4]Binary method is used for the genes where if a security control is selected (1) or not (0).

that chromosome meets the criteria or it does not. If the latter condition holds, it simply decreases the percentage of selected genes for further attempts. The iteration continues until the algorithm creates the required number of initial chromosomes. Once all chromosomes are initialized, the next step is to sort them based on their weight (Equation 3.15), which will be further divided into 2 parts; good (first part of a population with a given percentage) and bad chromosomes (rest of the population). Once the initial population is created after the above-mentioned steps, the next important part of GA is the creation of a new population (algorithms 9 and 10), where they comprise crossover and mutation procedures with a merge function. We have improved the crossover technique by applying both two-points and single-point methods as are shown in Figure 3.2. In this regard, for the configuration part, one should set the percentage of them as an input. Also, we have adapted the Elitism technique [101],

Algorithm 7: The main function of the GA algorithm

```
1  Function(GASelection)
   Input: K, π, L⃗, F⃗, LIMIT
   Require:
2  LIMIT ∈ ℕ                                          // a constant value to run the GA
   Ensure: lowest expenditure := (F⃗ ⊙ ∏π(K_s|x)) × L⃗ + x
3  generateRandomChromosomes(chromosomes, POP_Num)    // generate initial population of
     chromosomes
4  sortByExpenditure(chromosomes)          // sort chromosomes by expenditure from lowest to
     largest
5  theAnswer := chromosomes[0]                                  // Initializing theAnswer
6  for i := 1 to LIMIT do
7      chromosomes := CrossOver(nextGenChromosomes)                        // Call CrossOver
8      if theAnswer.expenditure < chromosomes[0].expenditure then
9          theAnswer := chromosomes[0]                  // ensuring the best chromosome
10     chromosomes := Mutation(nextGenChromosomes)                  // Call Mutation Function
11     if theAnswer.expenditure < chromosomes[0].expenditure then
12         theAnswer := chromosomes[0]                  // update the best chromosome
   Return: theAnswer
```

which allows us to copy some percentage of the population without per-

forming a crossover technique, to improve its effectiveness. Then, except E number of chromosomes, we add the rest of the population to a new list called *nextGenChromosomes*. Another contribution is that we classify the chromosomes by their weight (expenditure) and divide them into good and bad groups of chromosomes based on their performance. This new list of chromosomes will be further used for the crossover with 3 different combination methods – good with good, good with bad and bad with bad. The

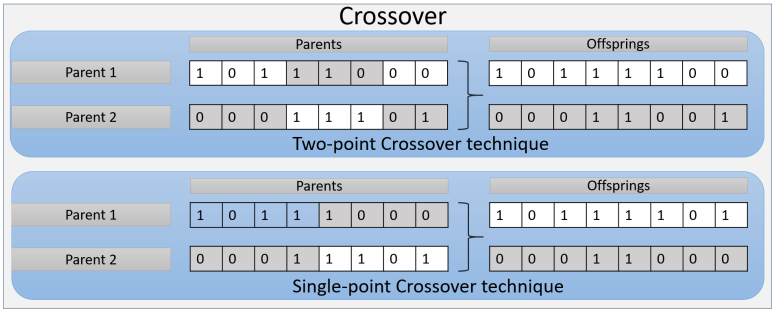


Figure 3.2: Crossover techniques

Algorithm 8: Merge Function for the GA

```
1  Function(Merge)
   Input: ch1, ch2, Y1, n_k
   Require:
2  Y1 ∈ ℕ                          // percentage of two-point CrossOver technique
3  ch1                                                  // a chromosome in a pair
4  ch2                                          // another chromosome in a pair
5  n_k ∈ ℕ                          // number of controls/genes in the chromosome
   Ensure: Merging two chromosomes ch1 and ch2
6  y = rand.range(0, 100)                               // some random percentage
7  if y <= Y1 then
8      l := rand.range(0, length(ch1.genes)-1)
9      r := rand.range(l, length(ch1.genes)-1)
10     for i := l to r do
11         ch1.genes[i] ↔ ch2.genes[i]          // swap i-th genes of two chromosomes
12 else
13     for i:=0 to n_k/2 do
14         ch1.genes[i] ↔ ch2.genes[i]          // swap i-th genes of two chromosomes
15 return ch1, ch2                                      // Return a pair of chromosomes
```

algorithm sorts the chromosomes after the crossover procedure (after line 28) to check whether the one we found is greater than the one we found before this step. In GA, a mutation process avoids the result falls into local minimum solutions and it helps to find the global optima. We have adapted the main concept of the mutation method, selecting random bits (number of random bits is defined in prior) based on a defined number, with the elitism technique, and reverse those bits as is shown in the Figure 3.3. The process takes place (see the Algorithm 10) after the crossover step by considering the offsprings, and sorts them by their weights to find the best performing one.

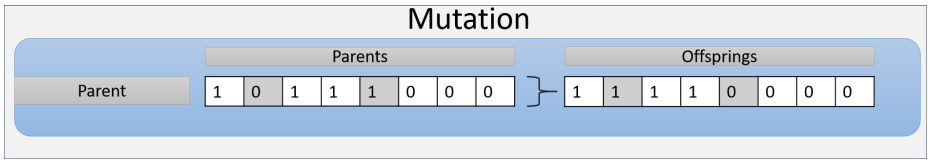


Figure 3.3: Mutation process

Algorithm 9: CrossOver function for the New Population of the GA

```
1  Function(Crossover)
   Input: chromosomes, x, N, LIMIT, Y2, Y3, b1, b2
   Require:
2  chromosomes                                          // a list of current chromosomes
3  N ∈ ℕ                                  // number of chromosomes in the population
4  b1 ∈ ℕ                          // crossover percentage of good and good chromosomes
5  b2 ∈ ℕ                           // crossover percentage of good and bad chromosomes
6  Y2 ∈ ℕ                           // percentage of chromosomes for Elitism techniques
7  Y3 ∈ ℕ                           // percentage of good chromosomes of the population
   Ensure: next Generation of Chromosomes obtained by CrossOver
8  nextGenChromosomes := []                          // Define nextGenChromosomes empty list
9  E := Y2 · N/100                          // Define the percentage of elitism in integer
10 for i := 1 to E do
11     nextGenChromosomes.append(chromosomes[i])      // Add i-th chromosome without doing
        crossover
12 r := Y3 · N/100                  // turn the percentage of good chromosomes into integer
13 for i := E+1 to N do
14     y := rand.range(0,100)                                  // define a random integer
15     if y <= b1 then
           // check if the crossover percentage of good chromosomes is greater than
           than a randomly chosen y
16         ii := rand.range(0, r)              // Define a random range of good chromosomes)
17         jj := rand.range(0, r)
18     else if y <= b1 + b2 then
               // check if the crossover percentage of good and bad chromosomes is
           greater than than a randomly chosen y
19         ii := rand.range(0, r)
20         jj := rand.range(r+1, N-1)                  // Random range of bad chromosomes
21     else
                // check if the crossover percentage of bad and bad chromosomes is
           greater than than a randomly chosen y
22         ii := rand.range(r+1, N-1)
23         jj := rand.range(r+1, N-1)
24     ch1, ch2 := Merge(chromosomes[ii], chromosomes[jj])
25     if ch1.cost < x or x = 0 then
                       // check if cost of ch1 is less than investment or equal to 0
26         nextGenChromsomes.append(ch1)
27     if ch2.cost < x or x = 0 then
                       // check if cost of ch1 is less than investment or equal to 0
28         nextGenChromsomes.append(ch2)
29 sort(nextGenChromosomes)                          // Sort the chromosomes by expenditure
   Return: nextGenChromosomes
```

Algorithm 10: Mutation function for the New Population of the GA

```
1  Function(Mutation)
   Input: chromosomes, Y2, b3
2  chromosomes                                          // a list of current chromosomes
3  N ∈ ℕ                                    // number of chromosomes in the population
4  Y2 ∈ ℕ                          // percentage of chromosomes for Elitism techniques
5  b3 ∈ ℕ                                        // defined number of bits to mutate
   Ensure: next Generation of Chromosomes (nextGenChromosomes) obtained by Mutation
6  nextGenChromosomes := []                  // Define nextGenChromosomes empty list
7  E := Y2 · N/100                  // Define the percentage of elitism as integer
8  for i := 1 to E do
9      nextGenChromosomes.append(chromosomes[i])                    // update the list
10 for i := E + 1 to N do
11     ch := chromosomes[i]
12     for j := 1 to b3 do
13         y := rand.range(0, length(ch.genes)-1)                   // reverse y-th gene in
14         ch[i].genes[y] := (ch[i].genes[y] + 1) mod 2                 // i-th chromosome
15     nextGenChromosomes.append(ch)                                // update the list
16 sort(nextGenChromosomes)                  // Sort the chromosomes by expenditure
   Return: nextGenChromosomes
```

3.4 Use Case Examples

In a competitive insurance market scenario, we have taken into account two different examples, artificial use cases and practical one which is a questionnaire-based risk assessment tool (see Chapter 4). For the former part, we compare the algorithmic solutions – DP, Greedy and GA, with various inputs. What we are interested in is the *execution time* of the proposed solutions and the dependency of input variables. The second crucial metric is the *accuracy* of solutions, in particular, approximate (Greedy and GA) solutions. It is obvious that the approximate algorithms will be much faster than the DP solution, however, we would like to observe the projection idea result comparing with the others. In terms of accuracy, DP based solutions unequivocally outperform the approximate solutions even though they struggle to find the answers in a preferable time when there are some large or complex inputs. Since it is time-consuming for DP solutions to run with those inputs, we set the time limits (assuming that there is no need to keep running after enough time spent) for the algorithms to finish. Therefore, we take a simple assumption, where we run the approximate solutions many times (i.e., high and most accurate settings) so that we can select the one that we receive most of the time. One may argue that the answer has the potential not to be the optimal one. On the other hand, the answer is capable of the nearest solution at least and it is the best reasonable check we can do. To check with different inputs, we have generated a small supporting program that generates the different types of inputs. The program does not fully randomly generate the inputs but with controlled, i.e., it depends on some quantitative and qualitative inputs parameters.

In more details, the quantitative approach for the input parameters comprises the *number of considered security controls* and *threats*, and we would like to investigate how the increase of numbers affect both execution

time and accuracy of the solutions. The qualitative input parameters, on the other hand, define the complexity of the inputs. The first parameter is the *Greatest Common Divisor (GCD)* determines the granularity of the search for an applicable solution (it is expected to easily compare and find the answers when GCD is higher). *Range of the control costs*, i.e., how big is the gap of controls' costs, would also affect the algorithms' result. The *number of threats affected by a control* shows how the countermeasure reduces the number of threats, and thus, potentially, this parameter could have an impact on the projection idea.

Experimented machine's technical preference. We have used an (Intel(R) Core(TM) i7-8550U CPU @ 1.80GHz (8 CPUs), 2.0GHz) machine that runs Windows 10 operating system for all the experiments. We agree on the performance of more powerful machines, which will yield the result in a shorter time, however, the absolute goal is to study the dependencies.

3.4.1 Basic and Simple scenario

We start with a simple example in order for a thorough understanding of how the proposed solutions work. Let's consider an organisation which has some available security controls to select from and identified possible threats whose corresponding single loss expectancies are:
$\vec{L} = \langle 3000, 1800, 2800, 4000, 3800 \rangle$. Totally eight controls ($|K| = n_k = 8$) are readily available to be installed and their costs are: ($c(k_1) = 480$; $c(k_2) = 240$; $c(k_3) = 120$; $c(k_4) = 80$; $c(k_5) = 200$; $c(k_6) = 120$; $c(k_7) = 280$; $c(k_8) = 200$). Furthermore, the organisation might have already installed some security controls that provide the initial probability of attack $\vec{p}_{init}$ and the expected frequency of threats $\vec{F}$. The probability of survival for each security controls $\vec{\pi}_j$ is also shown in Table 3.1. After implementing all the approaches with the above-mentioned input, we obtain the best controls

$\vec{p}_{init}$	$\vec{F}$	$\vec{\pi}_{k1}$	$\vec{\pi}_{k2}$	$\vec{\pi}_{k3}$	$\vec{\pi}_{k4}$	$\vec{\pi}_{k5}$	$\vec{\pi}_{k6}$	$\vec{\pi}_{k7}$	$\vec{\pi}_{k8}$
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 3.1: Input vectors

that keep the security expenditure at a minimum. The result is the same for all algorithms in terms of accuracy and has a trivial difference in time-consumption.

We first apply our approach based on dynamic programming which starts with an initial expenditure of *exp* equal to 5986. This expenditure will be our first limit for searching for the optimal investment level. Naturally, $\bar{p}(K_i|x))$ equals to vector $\bar{p}_{init}$ in the beginning. The minimal premium is equal to $P^*_{min} = 136$. Table 3.2 contains the result for the first 21 rounds of the algorithm. In the first round, the expenditure increases

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 3.2: Selection of best countermeasures within security investment

by the investment increment $C = 40$ since there are no countermeasures of the cost below the current investment level $x = 40$. After the first two rounds of investments ($x = 2 * C = 80$), we find the first viable 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 the 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 $x = 80$, $x = 320$ 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. Thus, our DP algorithm (see Figure 3.4) successfully avoids falling into local minimums (i.e., for $x = 80$, $x = 320$ or $x = 560$) and finds the optimal security investments, which is the global one, at $x = 760$. If the organisation invests

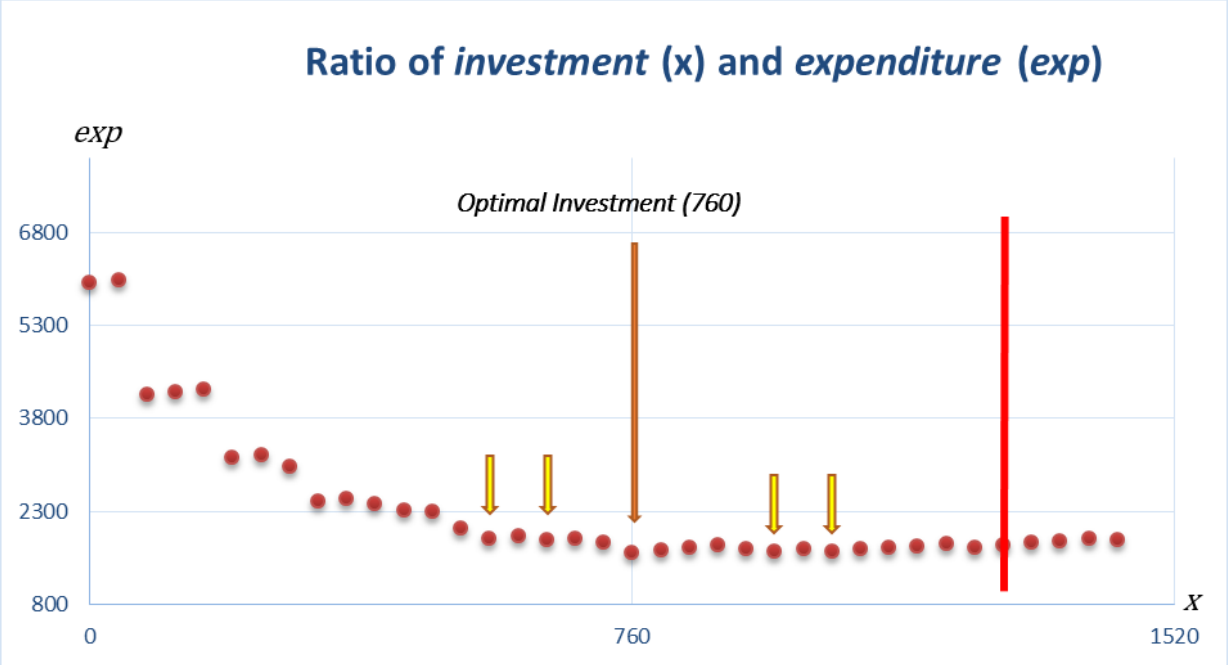


Figure 3.4: (Exp) expenditure for security self-investments x

760 for security controls $\{k_2, k_3, k_4, k_6, k_8\}$, the overall expenditure will be 1642. In Figure 3.4, it is also clear that after the optimal value, the overall expenditure (exp) is gradually increasing with some small drops until the iteration stops. This shows that, even though there could be some controls to reduce the risk, there are no cost-efficient ones to select. In this regard, DP-based algorithms simply check the limit and stop running at $x = 1280$.

For approximate solutions, Greedy and GA, the result is exactly the same as it is expected because the current input is relatively simple. While

DP checks all possible solutions through a series of iteration, the approximate algorithms stop as soon as they find the best controls based on their initial configurations, i.e., we set the *population number* and *round of iterations* for GA before start running.

3.4.2 Quantitative input parameters

Let us make the experiment more complex like it is similar to the real-life case by adding first more threats to the input. We would like to analyse the impact of several threats on the result of the proposed algorithms. The inputs are randomly generated with 20 security controls, 40 GCD (Greater Common Divisor - the gap between costs), the cost ranging from 80 up to 400, and each control affecting every threat. In this section, we would like to set the "high" values for the GA settings (see Table 3.3), yet, these values could be varied depending on the goal of the experiment, especially, for the qualitative analysis. Table 3.4 shows the results of experiments in

					chromosomes combination		
Mutation	Limit	Population size	Two point crossover percentage	Elitism percentage	Good & Good	Good & Bad	Bad & Bad
1 bit	1000	1000	80%	15%	50%	45%	5%

Table 3.3: Constants for GA execution

numeric values.

The first analysis is to find the dependency of the required time with the different number of threats n_t (see Figure 3.5). As it is expected, the execution time for the Greedy algorithm does increase while it grows for the other solutions with the increase of the threats' number. Comparing with GA, DP solutions take a much longer time where projection idea performs better than the original DP solution where its time increases

Table 3.4: Both Time&Accuracy of the solutions for increasing number of threats

		Number of threats	**5**	**10**	**15**	**20**	**25**	**30**	**35**	**40**	**50**
20 controls and up to 50 threats	**DP**	*Execution time (sec)*	0.3s	1.6s	16.7s	80.5s	323s	756.5s			
		Overall loss	800.2	825.4	963.6	1140.5	1213.8	1306.5			
	Projection	*Execution time (sec)*	0.1s	0.2s	0.7s	6.8s	8.9s	18.1s	27.4s	58.5s	271.9s
		Overall loss	800.2	825.4	963.6	1140.5	1213.8	1306.5	1479	1617.8	1638.9
	Greedy	*Execution time (sec)*	0.01s	0.014s	0.021s	0.015s	0.008s	0.009s	0.0156s	0.016s	0.015s
		Overall loss	**914.3**	825.4	**1045.2**	1140.5	1213.8	**1317.1**	**1560.1**	1617.8	1638.9
	GA	*Execution time (sec)*	2.8s	3.7s	5.1s	6.9s	8.5s	9.7s	10.9s	14.1s	16.4s
		Overall loss	800.2	825.4	963.6	1140.5	1213.8	1306.5	1479	1617.8	1638.9

exponentially with the increasing number of threats. Among four proposed

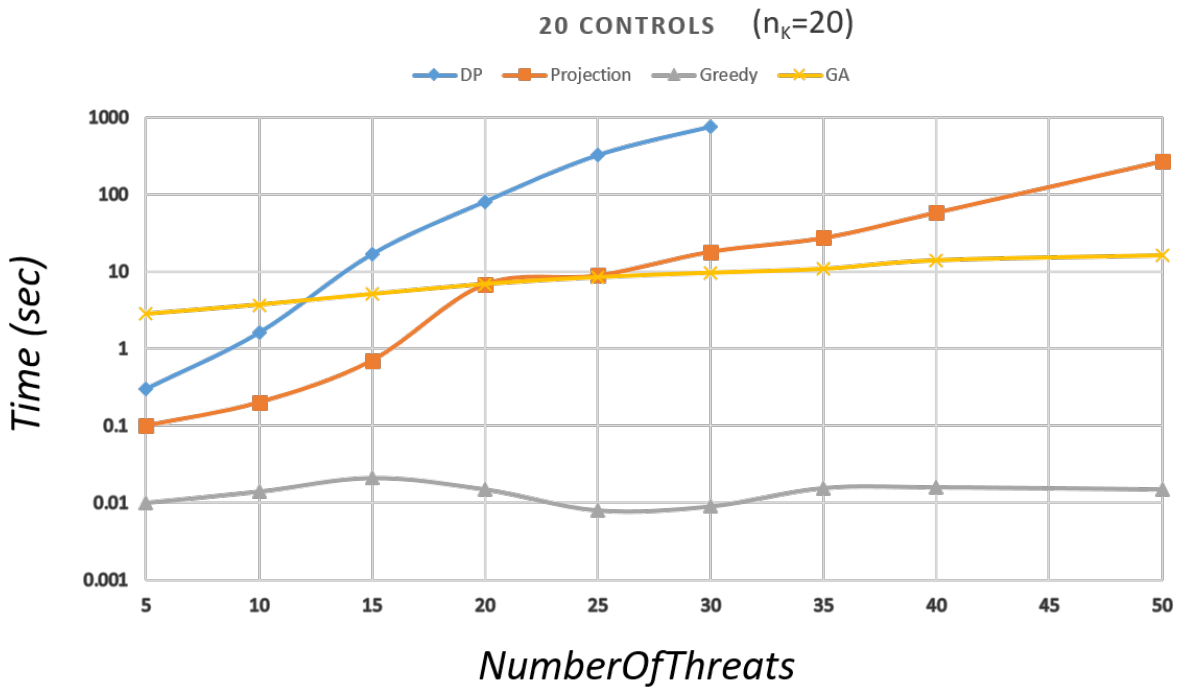


Figure 3.5: Comparison of execution time for 4 solutions in case of increasing number of threats with 20 control cases

solutions, the Greedy outperforms in terms of execution time, yet, it often fails (highlighted as ***bold*** in Table 3.3) to find the optimal answer. Another approximate solution, GA, performs well in this scenario with the "high" setting.

Furthermore, we would like to investigate the dependency of the execution time depending on the increasing number of controls. As opposed to the previous case, in these 4 experiments, the number of threats is fixed in each case $n_t = 5, 10, 15$ and 20. The four graphs in Figure 3.6 represent the results of the time dependency while the Table 3.5 indicates both time and accuracy of the solutions. Same as it was for the previous experi-

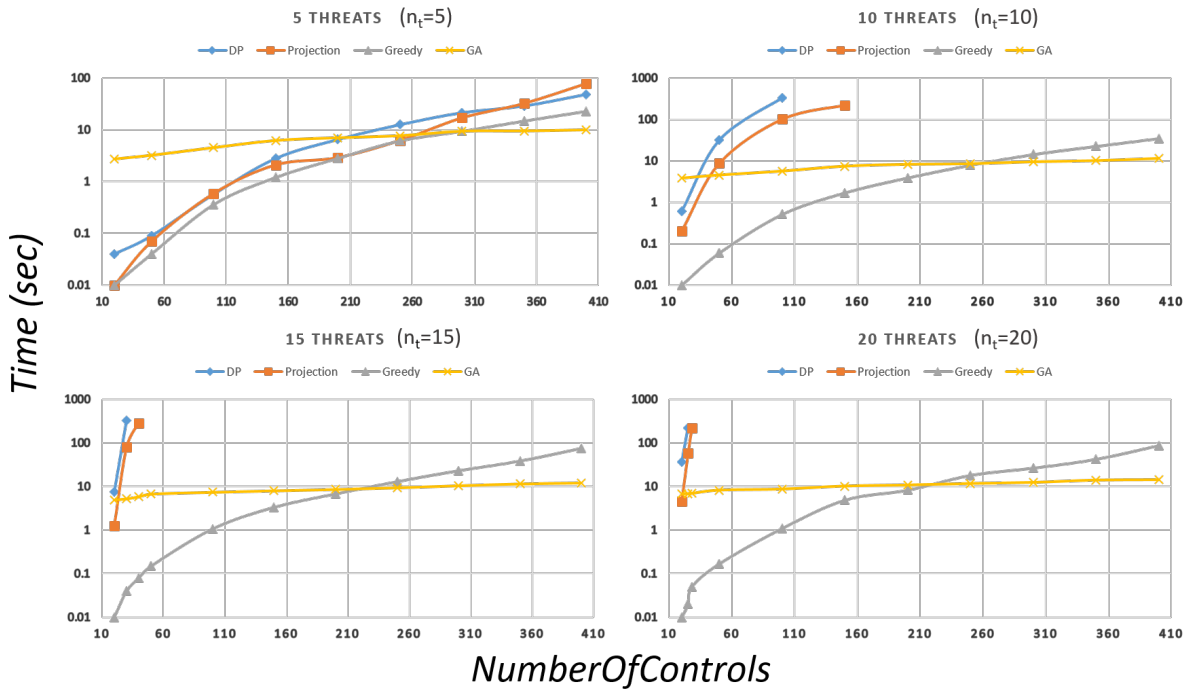


Figure 3.6: Comparison of execution time for 4 solutions in case of increasing number of controls with 5, 10, 15, 20 threats cases

ments, DP is the slowest and most affected by the increasing number of security controls. In particular, when the number of threats is increased, the execution time is relatively higher with the number of controls n_K. On the other hand, the improved DP solution is much faster than the ordinary DP algorithm although the difference is not comparable with the approximate solutions. The most interesting scenario is the increasing execution time for Greedy which was faster in terms of increasing numbers of threats.

Table 3.5: Both Time&Accuracy comparison for increasing number of controls

		Number of Controls	**20**	**50**	**100**	**150**	**200**	**250**	**300**	**350**	**400**
5 threats case with increasing number of controls	*DP*	*Execution time (sec)*	0.04s	0.09s	0.57s	2.8s	6.5s	12.6s	21.4s	28.9s	48.3s
		Overall loss	510.6	359.6	356.9	329.3	322.3	322.3	322.3	322.3	322.3
	Projection	*Execution time (sec)*	0.01s	0.07s	0.59s	2.1s	2.9s	6.2s	16.9s	32.1s	77.4s
		Overall loss	510.6	359.6	356.9	329.3	322.3	322.3	322.3	322.3	322.3
	Greedy	*Execution time (sec)*	0.01s	0.04s	0.36s	1.2s	2.8s	6.1s	9.3s	14.7s	22.6s
		Overall loss	510.6	**413**	356.9	**353.7**	**337.9**	**337.9**	**337.9**	**342.8**	**363.7**
	GA	*Execution time (sec)*	2.7s	3.2s	4.5s	6.2s	7s	7.69s	9.4s	9.5s	10s
		Overall loss	510.6	359.6	356.9	329.3	322.3	322.3	322.3	322.3	322.3
10 threats case with increasing number of controls	*DP*	*Execution time (sec)*	0.6s	31.9s	331.4s						
		Overall loss	850.1	553.7	468.1						
	Projection	*Execution time (sec)*	0.2s	8.7s	101s	220.7s					
		Overall loss	850.1	553.7	468.1	428.6					
	Greedy	*Execution time (sec)*	0.01s	0.06s	0.51s	1.7s	3.9s	7.9s	14.3s	22.5s	34.8s
		Overall loss	850.1	**562.7**	**488.3**	428.6	416.5	385.1	**422.3**	**422.3**	**455.3**
	GA	*Execution time (sec)*	3.77s	4.48s	5.6s	7.4s	8.2s	8.5s	9.5s	10.1s	11.5s
		Overall loss	850.1	553.7	468.1	428.6	416.5	385.1	385.1	385.1	385.1
15 threats case with increasing number of controls	*DP*	*Execution time (sec)*	7.6s								
		Overall loss	977								
	Projection	*Execution time (sec)*	1.24s								
		Overall loss	977								
	Greedy	*Execution time (sec)*	0.01s	0.15s	1.06s	3.31s	6.7s	12.8s	22.7s	37.8s	74s
		Overall loss	977	**834.2**	598.8	**599.2**	466.4	**478.4**	**488.5**	**471.9**	**441.9**
	GA	*Execution time (sec)*	4.9s	6.7s	7.4s	8s	8.6s	9.4s	10.5s	11.6s	12.2s
		Overall loss	977	789.7	598.8	576.2	466.4	466.4	468.5	465.2	434
20 threats case with increasing number of controls	*DP*	*Execution time (sec)*	36.7s								
		Overall loss	1236.2								
	Projection	*Execution time (sec)*	4.6s								
		Overall loss	1236.2								
	Greedy	*Execution time (sec)*	0.01s	0.17s	1.1s	4.9s	8.3s	18.1s	26.6s	42.3s	87.5s
		Overall loss	1236.2	850.9	**774.2**	**699.2**	**678.6**	**645.3**	**653.8**	**667.7**	577.9
	GA	*Execution time (sec)*	6.7s	8.2s	8.7s	10.2s	10.8s	11.7s	12.4s	14s	14.3s
		Overall loss	1236.2	850.9	714.2	659.1	642	619.2	619.2	612.1	577.9

Moreover, GA is less affected among all solutions, it is expected to keep the performance for the further increase of controls.

For accuracy, GA outperforms the Greedy solution which fails most of the time. However, at some points, it is hard to say whether GA finds the optimal solution since DP based algorithms cannot provide the result due to its prolonged execution time. In this regard, we run the experiment several times to ensure the result is the optimal or the nearest optimal at

least.

To conclude the quantitative analyses, the projection idea improves the original DP solution, yet, it is not enough when the number of parameters increases. On the contrary, the approximate solutions are much faster and especially GA is capable of finding the optimal solutions. For Greedy, regardless of its quick execution, it often finds the nearest solutions instead of the optimal ones. So far, GA with "high" settings is the most preferable solution for finding the optimal answer.

3.4.3 Qualitative parameters

While we showed how changing numbers of threats and controls affect the result, this part presents how the complexities of inputs qualitatively change the results. To conduct the qualitative analyses, we run at least 3 experiments with different values for the selected parameters (GCD, Range of the control costs, Number of threats affected by a control). These parameters make the computation more difficult for finding the optimal solution in approximate algorithms while DP becomes much slower. Apart from those parameters, the rest of the inputs stays constant for the experiment. The overall results can be given as are in Table 3.6.

For the controls and threats, the numbers are set at 30 and 10 respectively, and the costs are varied with different GCDs (40, 20, and 10) while the range of costs is between 80 and 160. According to the result, it is clear that DP algorithms are enormously affected by the decrease of GCD whereas approximate ones are less impacted by the change. The Greedy algorithm outperforms in terms of execution time, yet, it lacks accuracy comparing with others.

Furthermore, we present how the variation of costs can change the execution time of proposed solutions (see Table 3.6). Same as the first case, DP-based algorithms again are time-consuming as the variance becomes

		Algorithms	**DP**	**Projection**	**Greedy**	**GA**
Changing GCD (30 controls and 10 threats with 80 to 160 cost range)	**40 GCD**	*Execution time (sec)*	418s	74.6s	0.03s	3.8s
		Overall loss	627.1	627.1	**700.6**	627.1
	20 GCD	*Execution time (sec)*	496s	75.5s	0.03s	4.2s
		Overall loss	543.9	543.9	**567.8**	543.9
	10 GCD	*Execution time (sec)*	1369.6s	92.1s	0.03s	4.8s
		Overall loss	576.9	576.9	**613.2**	576.9
Different range of cost (30 controls and 10 threats with 40 GCD)	**80 - 400 range**	*Execution time (sec)*	6s	1.2s	0.01s	3.6s
		Overall loss	706.6	706.6	706.6	706.6
	80 - 160 range	*Execution time (sec)*	418s	74.6s	0.03s	3.8s
		Overall loss	627.1	627.1	**700.6**	627.1
	80 - 120 range	*Execution time (sec)*	1741.7s	132.5s	0.03s	4.2s
		Overall loss	495.3	495.3	**544.2**	495.3
Affected threats (30 controls and 10 threats with 40 GCD and 80 to 400 cost range)	**1 threat**	*Execution time (sec)*	>600s	0.2s	0.01s	4.7s
		Overall loss		10277	10277	10277
	4 threats	*Execution time (sec)*	>600s	3.3s	0.01s	3.8s
		Overall loss		2411.5	2411.5	2411.5
	7 threats	*Execution time (sec)*	339.9s	1.7s	0.01s	3.6s
		Overall loss	947.2	947.2	947.2	947.2
	10 threats	*Execution time (sec)*	6s	1.2s	0.01s	3.6s
		Overall loss	706.6	706.6	706.6	706.6

Table 3.6: Both time and accuracy of the solutions for different scenarios

lower. For the approximate ones, they yield the result in a bit longer time comparing to the previous example of changing GCD. As it is expected, the Greedy one is the worst for finding the optimal answer.

The final experiment is to study the situation when controls work against only a certain number of threats (e.g., 1, 4, 7, and 10). The fewer threats are affected, the more time required for the original DP approach, while GA and DP with projection solutions' time gradually drops. In this experiment, we clearly see how DP with projection idea improves the original approach as it finds the solution much faster for 1 threat affected case and immediately increases for 4 threats affected case. This can be explained that the projection idea is much effective with non-dominated vectors, especially, when those are easy to project. The good thing is that the Greedy

solution is stable with execution time at around 0.01 seconds and finds the optimal solutions.

3.4.4 Precision of GA and Greedy algorithms

In previous experiments, it has been presented that the approximate solutions, Greedy and GA, are much faster than DP ones for finding the solution. However, at some points, they are inaccurate when the input becomes more complex or large. In plain words, it can be concluded that the approximate solutions may produce the optimal answer unless it is tested with different inputs to know their limits. In this regard, we have changed the settings for GA from "high" to different levels (i.e. lowering the limit number and population size). In Table 3.7, we evaluate the execution time and accuracy of the algorithms with different settings for GA and their comparison with the Greedy results (binary representation of either *Success* or *Failure* for finding the optimal answer). Since the accuracy of GA cannot be proved, we have run the experiment 10 times (highlighted and represented in seconds) for each case for GA ones.

With the small population size and limit, GA fails more often to find the optimal solution even though it is much faster than the "high" settings[5]". Same as the qualitative analyses, some parameters affect the accuracy and time, i.e., GCD and Range of costs. It is also conceivable that the gap between results is not huge. For instance, when the range of costs is between 80 and 160 while the limit and population size are set at 100, there are 4 different outcomes whose difference are 29.4 (about 5% difference with the optimal answer) utmost.

Naturally, the Greedy solution is much faster producing the result, and it fails most of the time.

[5] "High Settings" for GA represents a larger number of population size and the round of iteration (limit)

		Genetic Algorithm										Greedy
		Limit number	**100**			**500**			**1000**			
		Population size	***100***	***500***	***1000***	***100***	***500***	***1000***	***100***	***500***	***1000***	
Increasing number of controls (20 threats 40 gcd with range of 80 to 400 costs)	**20**	*Execution time (sec)*	0.1	0.3s	0.5s	0.2s	1.1s	2s	0.5s	1.8s	3.8s	0.03s
		Overall loss	10/10	10/10	10/10	10/10	10/10	10/10	10/10	10/10	10/10	**Success**
	50	*Execution time (sec)*	0.1s	0.3s	0.6s	0.3s	1.2s	2.3s	0.5s	2.2s	4.2s	0.2s
		Overall loss	8/10	10/10	10/10	10/10	10/10	10/10	10/10	10/10	10/10	**Failure**
	100	*Execution time (sec)*	0.2s	0.7s	1.2s	0.7s	2.4s	4.6s	1.1s	4.5s	9s	1.3s
		Overall loss	7/10	7/10	10/10	8/10	10/10	10/10	9/10	10/10	10/10	**Failure**
Increasing number of threats (50 controls 40 GCD with range of 80 to 400 costs)	**20**	*Execution time (sec)*	0.1s	0.3s	0.6s	0.3s	1.2s	2.3s	0.5s	2.2s	4.2s	0.2s
		Overall loss	8/10	10/10	10/10	10/10	10/10	10/10	10/10	10/10	10/10	**Failure**
	30	*Execution time (sec)*	0.2s	0.8s	1.4s	0.7s	2.6s	5.4s	1.2s	5.9s	10s	0.31s
		Overall loss	5/10	10/10	10/10	8/10	10/10	10/10	10/10	10/10	10/10	**Failure**
	40	*Execution time (sec)*	0.2s	1.1s	1.8s	0.9s	3.7s	7.2s	1.7s	7.3s	14s	0.38s
		Overall loss	2/10	5/10	8/10	3/10	9/10	10/10	8/10	10/10	10/10	**Failure**
Different GCD (50 controls and 20 threats with range of 80 to 400 costs)	**40 GCD**	*Execution time (sec)*	0.1s	0.3s	0.6s	0.3s	1.2s	2.3s	0.5s	2.2s	4.2s	0.2s
		Overall loss	8/10	10/10	10/10	10/10	10/10	10/10	10/10	10/10	10/10	**Failure**
	20 GCD	*Execution time (sec)*	0.1s	0.3s	0.6s	0.3s	1.2s	2.3s	0.9s	3.8s	7.4s	0.2s
		Overall loss	5/10	10/10	10/10	7/10	10/10	10/10	9/10	10/10	10/10	**Success**
	10 GCD	*Execution time (sec)*	0.1s	0.3s	0.6s	0.3s	1.2s	2.1s	0.6s	2.2s	4.1s	0.21s
		Overall loss	5/10	9/10	10/10	10/10	10/10	10/10	10/10	10/10	10/10	**Failure**
Different range of cost (50 controls and 20 threats with 40 GCD)	**range of 80 - 400**	*Execution time (sec)*	0.1s	0.3s	0.6s	0.3s	1.2s	2.3s	0.5s	2.2s	4.2s	0.2s
		Overall loss	8/10	10/10	10/10	10/10	10/10	10/10	10/10	10/10	10/10	**Failure**
	range of 80 - 240	*Execution time (sec)*	0.1s	0.3s	0.6s	0.3s	1.2s	2.2s	0.5s	2.2s	4.3s	0.2s
		Overall loss	3/10	8/10	8/10	5/10	7/10	8/10	6/10	10/10	10/10	**Failure**
	range of 80 - 160	*Execution time (sec)*	0.1s	0.3s	0.6s	0.3s	1.2s	2.2s	0.5s	2.3s	4.2s	0.2s
		Overall loss	3/10	4/10	7/10	5/10	5/10	8/10	8/10	10/10	10/10	**Failure**
Affected threats (50 controls and 20 threats with range of 80 to 400 costs and 40 GCD)	**1 threat only**	*Execution time (sec)*	0.2s	0.8s	1.5s	0.7s	3.1s	6s	1.3s	6.1s	22s	0.03s
		Overall loss	10/10	10/10	10/10	10/10	10/10	10/10	10/10	10/10	10/10	**Success**
	3 threats affected	*Execution time (sec)*	0.2s	0.6s	1.3s	0.6s	2.8s	5s	1.1s	5.1s	18s	0.06s
		Overall loss	5/10	10/10	10/10	10/10	10/10	10/10	10/10	10/10	10/10	**Failure**
	7 threats affected	*Execution time (sec)*	0.1s	0.5s	0.9s	0.5s	1.9s	3.6s	0.9s	3.5s	7s	0.09s
		Overall loss	4/10	7/10	10/10	6/10	10/10	10/10	8/10	10/10	10/10	**Failure**

Table 3.7: Different configurations for GA solution and their comparison with Greedy

3.4.5 Analysis of results with artificial cases

With the consideration of about 10-20 threats and for 50-100 controls without any complex parameters, DP solution with projection is the most preferable as it is accurate and does not consume much time, where around 5-10 minutes are acceptable for a strategic decision for a long time (i.e., a year). Furthermore, the performance will definitely be improved with more advanced methods (i.e., parallel computations) and running on powerful machines. It is also faster than GA solution in the case of small inputs. On the other hand, if one has a list of full sets of controls e.g., NIST [9] or ISO-27002 [75] to select and more potential threats (e.g., see ISO 27005

[98], DP-based solutions are not offered over approximate solutions.

Last but not least, not only does the quantity affect the result, but the quality also has the capability of leading to different results. In this regard, depending on what situation and tipping-points lying, the solutions can be selected. It also can be seen that the GA solution with "high" settings can be applicable for most of the cases to find the optimal solution in an applicable time.

3.5 Discussion and Limitations

This section discusses some limitations considered in this chapter, particularly related to its practical application.

We first underline that the work is based on a competitive insurance market model, which is considered simple to conceptualise and often used for theoretical analyses [94, 95]. The incentive of using the model is to simplify the analyse and focus on the core problem. From a practical perspective, we acknowledge that such a model requires various supports, i.e., government regulations, to keep its stability. We often see a dominant or non-competitive insurance market in real life, where the premium is computed higher than it is in the competitive insurance market model due to the additional loading factors [25]. Moreover, since our analysis further involving the multi-threats scenario, we first aim for a convincing result so that we will be able to move into future investigations. We believe that even in the competitive insurance market, our contribution will be a crucial step to encourage further analysis.

The cost of security controls is considered independently from the efficacy of them. Some may claim that some security controls require the presence of another control (e.g., security audit may require the presence of monitoring and logging mechanisms) or even conflict with each other

(e.g., cryptography may reduce the effectiveness of security audit). We considerably agree on the aspect and already started working on further resolutions. Some issues can be resolved by adjusting the input data (e.g., grouping some controls) and others can be caught by extending our core algorithms.

We admit that our proposed approach surely depends on knowing the probability of survival (security control ability) and expected losses triggered by threats. These values are difficult to find or compute due to the lack of statistical data we rely on or we can obtain [108]. From the empirical data point of view, we believe that cyber insurers are becoming more capable of finding these values since they collect more data from the customers as this market becomes mature. One of the alternatives for acquiring the value of threat survival is that we integrated the time-to-compromise metric with our model (see Chapter 5.1). Even though the idea is not still completely proven, we believe that similar ways of looking at the problem could be applied. Also, some researchers conducted Capture The Flag (CTF) experiments to measure the efficacy of security controls as well as the attacker's level of skills. In terms of estimated losses, we see some positive results from IBM Security and Ponemon institute as they report statistics [7] of cyber-related losses depending on the security controls installed.

3.6 Summary of the chapter

In this chapter, we theoretically analysed the security expenditure distribution problem for a risk-averse organisation which expects multiple-threats in a certain period and has a cyber insurance option as a backup risk treatment alternative. We have conceptually modelled the competitive insurance market and found out that even in the presence of several threats,

the market leads to full insurance coverage as an optimal solution.

The proposed approach further helps the organisation to make a cost-efficient decision on selecting the best security controls, which eventually leads to optimal investments for the self-protection and cyber insurance premium. Our solution provides the opposite insight from the traditional methods (i.e., selecting the controls in a defined budget) and can be adapted depending on the organisation's goal.

Based on our theoretical analysis, we have provided algorithmic approaches to find both exact and nearest-optimal answers to the problem. Our exact algorithms (Dynamic programming and Projection idea) are suitable for a small and medium number of controls and threats. On the other hand, the approximate algorithms are preferable for a large number of inputs since they are comparably faster than the exact algorithms. In particular, the Genetic Algorithm outperforms the greedy approach in both qualities of finding the optimal answer and even speed in some cases.

Chapter 4

Risk assessment tool based validation

As we proposed our security expenditure distribution solution for risk treatment options in the previous chapter (in Chapter 3), we further integrated the solution with a practical case where we have developed a risk assessment (hereinafter RA) tool to obtain the input information for our proposed solution. The whole process is to assess the risk and define both installed and available security controls to implement so that we will be able to find the best set of security controls with the optimal investments and offer the minimal premium.

To integrate our proposed solution with the RA tool, we need the following information as an input for the optimisation solution.

- Number of available security controls,
- Number of potential threats,
- Cost and efficacy of each control,
- Single Loss expectancy depending on each threat.

This information can be fully acquired based on the RA tool except for the cost of controls, which requires more practical and plausible reasons to

define. For the validation purpose, we have defined the costs considering some public scenarios, i.e., the implementation cost of security controls. Also, our developed RA tool has the option that each user/organisation can provide their own expected cost for implementing each security control. By applying the latter notion, we give the organisation chance to control the costs of security controls, and only then, our solution for risk treatment options will be applied.

Before we start introducing our integration procedure and result, we explicitly deliver the background notion of our RA tool. We have not addressed any innovative approach for the tool since the RA part was not our main goal in this thesis. However, the main goal is to obtain complete information on an organisation's security posture and provide experts with the full information to make a rational decision on efficiently distributing the security expenditure on risk treatment options. Furthermore, it is worth noting that it could be any risk assessment method to be integrated with our treatment solution on the condition that it provides all necessary inputs to our tool.

In most literature and guidelines, i.e. [111, 8, 12], the risk assessment process has been done by considering the following main procedures; identifying assets, vulnerabilities and potential threats, as well as estimating the likelihood of attacks and impact of incidents. Some researchers, i.e., [12, 8, 13], introduced a method for identifying and assessing the risk based on several meetings, workshops, and interviews with stakeholders. Also, the questionnaire method was introduced as an alternative method of collecting information and knowing the current state of the organisation [14, 15]. The latter approach is often considered, especially, in the cyber insurance case, insurers mostly come with a set of questions to calculate the premium. *We derive the idea of the questionnaire approach in this work to collect the information to assess the organisation's risk. The set of ques-*

tions is created by using ISO/IEC 27001 standard and its security controls to have the complete questionnaire for checking whether an organisation meets the baseline security requirements.

4.1 RA tool

To give the main idea of the RA tool, let's start with the methodology we adopted for computing the probability of attack. Every question (Example is in Figure 4.1) is comprised of a certain category depending on its goal. Moreover, each question has its answers, either those are binary or multi-selection ones. The main method to compute the probability of an attack is the adoption of a weighted approach, where each answer represents the value which can be seen as the effectiveness of corresponding controls to block specified threats or close the vulnerabilities. Definitely, defining and linking the values to those answers require sophisticated methods or well-managed empirical data. To beat the odds, we have used the mining method for public reports and databases to obtain the values we needed for the initial start. The values will be more accurate with the availability of empirical data in future as we already acquired the statistical data from ADVISEN database [90]. So the probability of an attack is the inverse of security control's ability to block the threats, which can be called survival probability in this whole work. For the loss estimation, specific questions and category are dedicated to defining all assets of an organisation and the impact of those defined assets (in Figure 4.2) being compromised. We compute the loss of each assets depending on its damage to the CIA (Confidentiality, Integrity, Availability) and a number of assets. Thus, the computed costs of assets combined with the threat frequency will estimate the overall single loss expectancy an organisation may face during a certain period. Using the conceptual way of computing the risk, an

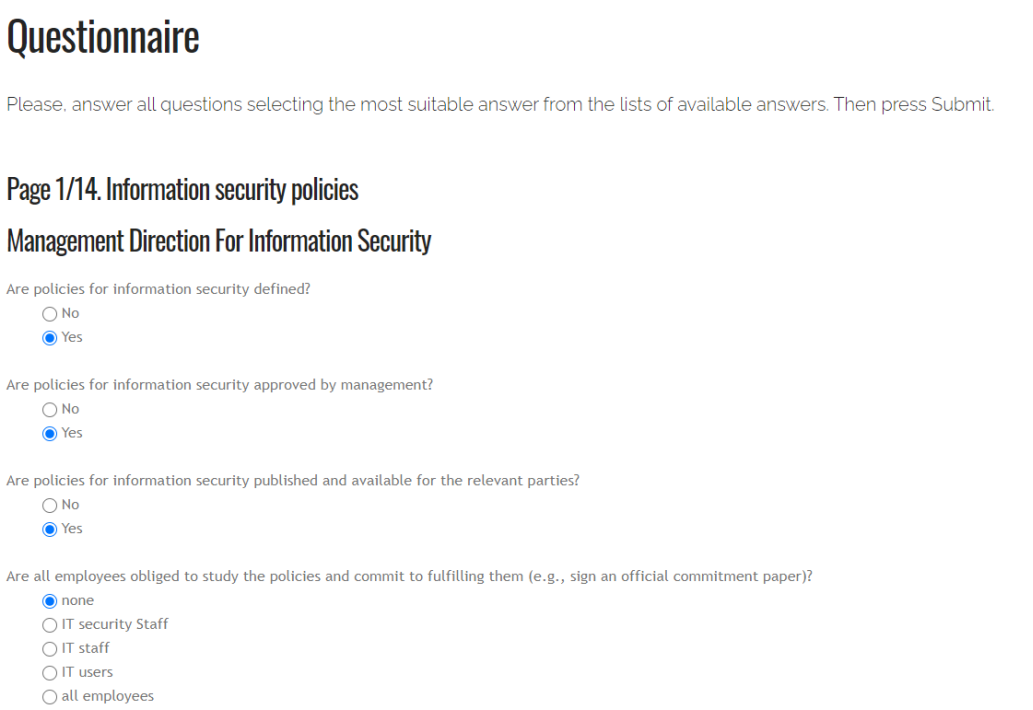


Figure 4.1: Example question of RA tool

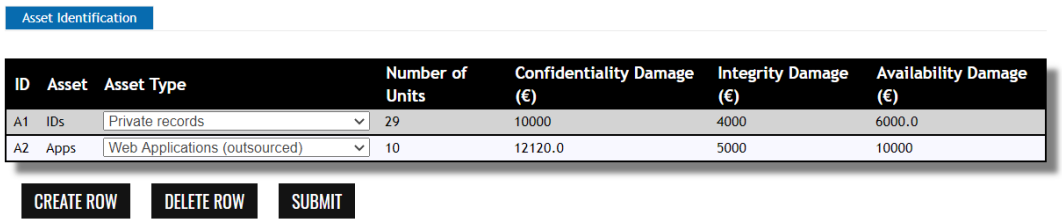
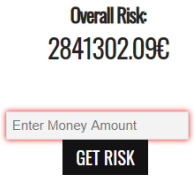


Figure 4.2: Example on asset identification of RA tool

organisation obtains the overall risk after completing the set of questions as is shown in Figure 4.3.

Basically, we obtain the overall risks of an organisation with a thorough detail of each threat's damage. Also, we acquire the information on what security controls are installed (in our case, questions that are answered *"Yes"*) and available security controls that can be considered for further improvements. Moreover, the result can provide more details on the impact and likelihood of each control and categories to make further decisions either to reduce or accept them.



Threat title	Risk
web application attacks	686535.97
malware	190010.08
Environmental damage	3007.1
Phishing	233386.08
Physical damage	637.16
System glitch	1038.61
Onsite penetration/tempering	198700.03
Communication break	713733.83
Malicious client	37465.45
(D)Dos	79442.38
Employee Negligence	40206.65
Insider Threat	28619.97
System inappropriateness	7317.32
Social engineering attacks	42165.62
Mechanical failure	1967.59
Hardware theft	110737.09
Third Party Problems	43121.69
web based attacks	211956.14
Spam/Infected email	0.0
ransomware	211253.22

Figure 4.3: Computed risks per threats and overall risks

4.2 Integration

In this section, we integrate our proposed solution with complete the risk assessment process. Once we assess the current risk, only then can we deal with the risks by conducting the most effective treatment approaches. What we need in our risk treatment solution (as we proposed in the previous chapter (Chapter 3)) is the required inputs. The only thing did we miss is the cost of each security controls which we found hard to convince the organisation to use our proposed costs for the controls. In this regard, we develop another additional step after the risk assessment process in which, only if want, an organisation fills the fields of expected costs for each available security controls (see Figure 4.4). The overall cost could consist of two main parts, implementation cost (working hour payment)

Questions	Answers	Budget
Are policies for information security defined?	Yes	
Are all employees obliged to study the policies and commit to fulfilling them (e.g., sign an official commitment paper)?	IT staff	
How often are the policies reviewed?	once in half a year	
Do candidates for employment pass cyber security screening?	IT security Staff	
Are there any special cyber security awareness and training activities for organisation employees?	IT staff	
Have the organisation identified its information assets?	once in half a year	
How often are the access control policies reviewed?	once in half a year	
How often do the asset owners review user's access rights?	once in half a year	
How many of the information and application system functions are (access) restricted in accordance with the access control policy?	20-30\%	
How many of the secure log-on procedures are required by the access control policy is in place?	20-30\%	
How many of the high quality authentication mechanisms are required by the access control policy are actually in place?	20-30\%	

Figure 4.4: Expected cost for available security controls

and physical cost to buy the security control (i.e., firewall). Once they fill these costs and provide us with an expected security investment the organisation would like to spend (optional), then our proposed solution shows the best security controls within the investment value they put. The example is shown in the following (Figure 4.5). In this example, we see the reduced risk after selecting the best security controls using our algorithmic solution we proposed within 1000$. The initial risk is reduced almost 60% after certain investments. As our proposed solution offers, the organisation can have no limit for the security expenditure and simply selects all efficient controls to install. In this regard, our solution reduced the risk by almost 95% from the initially estimated risks and spend 11600$ (See the Figure 4.6).

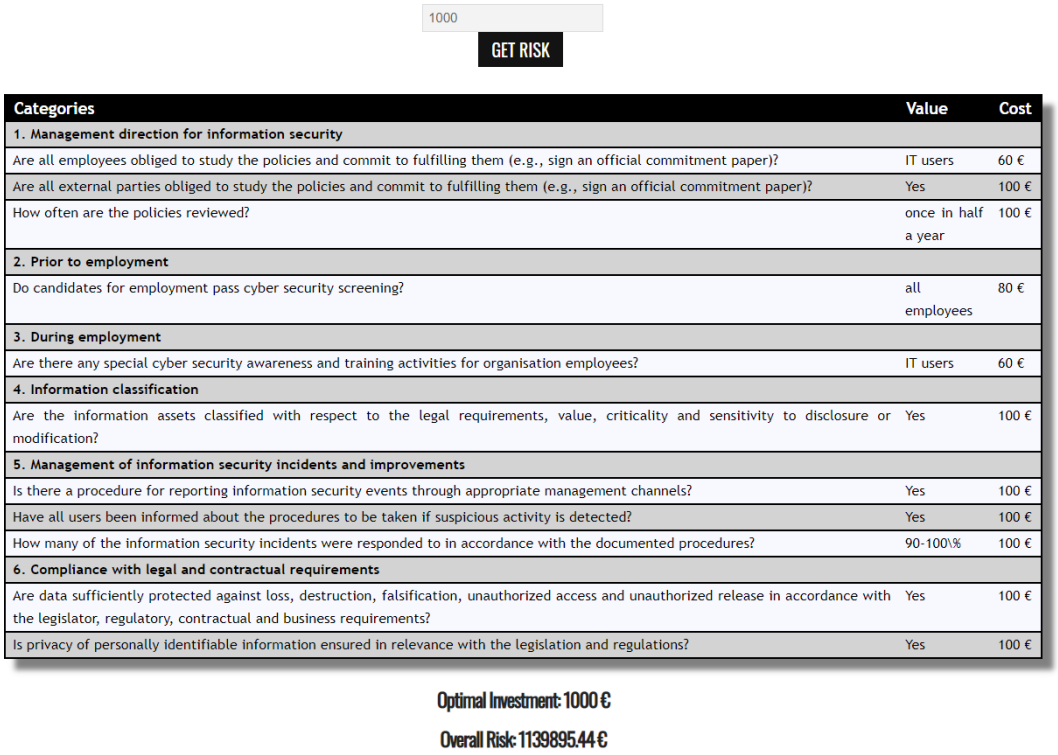


Figure 4.5: Reduced risk by implementing these controls within 1000$

Figure 4.6: Reduced risk by selecting the best controls with 11600$

4.3 Discussion

First, the probability of attack computation based on public data and reports. Then we have used a weighted approach to link the probability to a corresponding vulnerability and control. For future improvements, we would like to validate the values based on statistic data we have recently acquired from the ADVISEN database and information that organisations provide using our online tool.

We admit the costs of controls we initially set seem to be invalid and

not practical. We, therefore, show this version as a test and the costs can be changed either by us or the users. In this example, we would like to show how it works and the interoperability of developed tools.

Last but not least, the integrated tool does not distinguish the administrative, physical and logical controls but it has the capability to separate and propose the desired security controls. To that end, we only modify and extend the core algorithm.

4.4 Summary of the chapter

In this chapter, we have evaluated the potentiality of our risk treatment approach to be adapted in a practical case. To validate, we have developed the questionnaire-based risk assessment tool which uses the weighted approach to compute the risks after knowing the security level of an organisation. The main purpose is to integrate our risk assessment tool and treatment approach as a whole process.

For the integration, we additionally added a section that takes costs for each available security controls from a user. Thus, the treatment approach will be able to find the best security controls within the pre-specified budget or optimal security investments. As a result, we showed that our security expenditure distribution approach is capable of yielding promising result even in real-world cases.

We admit that the integration is at its initial phase and has plenty of room to improve in our further works.

Chapter 5

Advanced Properties

This chapter discusses two pertaining approaches under competitive insurance market analysis. We first introduce Time-to-Compromise metric as a supplementary method for computing the probability of attack and integrated it into our proposed solution. For the second properties, we investigated how security interdependence affects the security investments.

5.1 Time-to-Compromise metric

We would like to embed the time-to-compromise (TTC) metric into our security expenditure distribution solution for the following purpose:

- As an alternative and supportive method to find the efficacy of security controls, eventually the probability of attack.
- Propose a future direction for altering the usual period (one year) of the cyber insurance contract.

Elevating the security level is impossible unless we know the current level of security. Several researchers studied measuring the security level of organisations and they [17, 77, 19] proposed a solution based on the time-to-compromise metric to compute the probability of a successful attack. Let us denote V as the number of vulnerabilities that lie in the organisation

and t is the expected time to be compromised. Considering this information and current works [17, 77, 19], we would like to find the probability of attack $p(x)$.

So far, in our proposed solution, we assumed that the efficiency of security controls (probability of survival) can be found by mining the reports and public datasets. However, there is an applicable interconnectedness between our proposed solution and the time-to-compromise metric approach. *Thus the value of security controls is the capability of closing the vulnerabilities in the system. Based on this capability, we would like to find the expected time to compromise the system which leads to the computation of the probability of a successful attack.*

5.1.1 Formal Analysis

To conduct the analysis, let us start introducing the TTC approach which is based on the model of Mcqueen et al., [17] and mixed with the ideas of William et al., [19] to improve its applicability. To successfully compromise a system, there are 3 different phases to take place according to the authors:

1. Phase 1 - a system has at least one known vulnerability as well as an exploit is available for that, and the probability of an attacker compromises a system is denoted as $p_{v,exp}$.

2. Phase 2 - a system has at least one identified vulnerability to exploit but no known exploit is available, and the probability for this phase is $p_{v,noexp}$.

3. Phase 3 - is the identification of both unknown vulnerability and exploit, $p_{nov,noexp}$.

We use M as the number of known exploits and NVD is denoted as a non-duplicate set of vulnerabilities in the National Vulnerability Database.

$$
\begin{aligned}
& t = \tau_1 \cdot p_{v,exp} + (1 - p_{v,exp})(\tau_2 p_{v,noexp} + \\
& + \tau_3 \cdot (1 - p_{v,noexp}) p_{nov,noexp}) \qquad where \\
& p_{v,exp} = Pr\left[\exists known(v) \wedge has(i,v) \wedge exploit(v)\right] = \\
& = 1 - e^{-|V||M|/|NVD|}, \\
& p_{v,noexp} = Pr\left[\exists known(v) \wedge has(i,v) \wedge \neg exploit(v)\right] = \\
& = 1 - e^{-|V|/|NVD|}, \\
& p_{v,noexp} = Pr\left[\forall known(v) \neg has(i,v) \wedge \neg exploit(v)\right] = \\
& = (1 - s)^{|V|} \cdot e^{-|V||M|/|NVD|}, \qquad (5.1)
\end{aligned}
$$

where τ_1, τ_2, τ_3 represent the time required for each phases while $s \in [0, 1]$ indicates attacker's skill level depending on either novice, beginner, intermediate or expert. Also, the probability of finding the zero-day vulnerability is completely linked with the attacker's skill where the novice one takes the longest time than others. We also use $Pr\left[\exists known(v) \wedge has(i,v) \wedge exploit(v)\right]$ for the probability if there is a known vulnerability $v \in V$ in the organisation and there is an available exploit for this vulnerability and the attacker has it. Now, finding these 3 times (τ_1, τ_2, τ_3) is the pivotal step to compute the overall time-to-compromise t and the probability of successful attack $p(x)(t)$ (in our main solution it is a vector $\vec{p}(x)(t)$).

time 1 To find the required time, we have taken into account an experimental work conducted by Jonsson et al. [79] and the work of [19]. If there is a given vulnerability, it only takes 4 hours for 2 novice attackers to take down the system, which is 8 hours for one attacker. However, the success of compromising the system depends on the severity of the vulnerability

score which was proposed in [19]. So, the τ_1 is given:

$$\tau_1 = 1\ day \cdot \frac{10}{cvss(e)} \tag{5.2}$$

, where $cvss(e)$ represents the mean CVSS score of the vulnerabilities V 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 [18]. Yet, it becomes more accurate based on specific applications' needs.

time 2 The mean time τ_2 for phase two depends on the known vulnerability and the overall vulnerabilities in NVD. This scenario, without known exploits, excludes the novice and beginner attackers since this process takes higher skill sets. For those who are capable of creating an exploit, the chance of successfully attacking the system depends on the mean CVSS score. To know the average time, researchers take the mean time of announcing the new exploit for the vulnerabilities, which is around 5.8 days on average. Considering this time as a baseline, the time for phase 2 is given:

$$\tau_2 = 5.8\ days \cdot \frac{10}{cvss(e)} \tag{5.3}$$

time 3 If there is neither vulnerability nor exploit available, finding the time for phase 3 is a challenging task. In the formula proposed by Rescorla [78], taking the mean time for the next vulnerability announcement into consideration can be the solution for this phase. The authors empirically estimate the basic time as 30.42 days, for the time between new vulnerabilities. Also, the attacker's skill s is the crucial factor in this phase. N.Paulauskas et al. [77] proposed that beginner skill level s interval is to be between 0.1 to 0.6, intermediate between 0.6 to 0.8, and expert 0.8 to

1.

$$\tau_3 = ((1/s - 0.5) \cdot 30.42 + 5.8days) \cdot \frac{10}{cvss(e)}\ days \tag{5.4}$$

Finally, overall time-to-compromise t can be computed as the following way:

$$\begin{aligned} t = \tau_1(1 - e^{-|V_i||M_i|/|NVD|}) + \tau_2 e^{-|V_i||M_i|/|NVD|}(1- \\ - e^{-|V_i|/|NVD|}) + \tau_3(1-s)^{|V_i|}e^{-|V_i|(2|M_i|+1)/|NVD|}, \end{aligned} \tag{5.5}$$

where $\tau_1,\ \tau_2,\ \tau_3$ will be replaced as we computed using CVSS scores and mean times. Now the solution depends on the number of vulnerabilities in a system that can be decreased by efficient selection of countermeasures K_i.

5.1.2 Summary of the section

In Chapter 3, the probability of attack $\vec{p}(K_s|x)$ is computed based on the probability of a threat survival π. This work assumes that the values of threat survival probabilities are given. Without statistic data, finding these probabilities is not trivial. From the other perspective, we may find the value based on available information of the organisation. We simply deal with the vulnerabilities in our system and see the problem from a different point of view. Without an available vulnerability, a threat cannot survive through the installed controls. We, therefore, install the best security controls that can remove the vulnerabilities which cause the loss. Basically, if $\pi_k = 0.3$, the countermeasure removes 70% of all vulnerabilities $\vec{V}$. In this regard, we do not need to entirely modify our algorithms but play with some values and way of looking at the problem. Also, we could extend our work integrating with other's experimental works regarding the security controls' measurement based on CTF competitions.

Furthermore, we are interested in changing the contract period of cyber insurance in our future work. Some organisations claim that the premium is too expensive to have a cyber insurance option or they want flexible contracts in terms of timing. Also, one year can be a long period for some organisations to be attacked or it can be a short time for some in cyber security landscapes. Likewise other insurance areas, i.e., travel insurance, we would like to investigate if cyber insurance can derive the idea to provide different contracts. In this regard, the time-to-compromise metric can be a pivotal piece for such an analysis.

5.2 Effect of Security Interdependence in Competitive Insurance Market

Security interdependence is a vital external factor in the cyber landscape and it is rapidly increasing these days due to the interconnectedness of more devices, such as IoT and Cloud services [2, 3]. One's system can be attacked or data is breached through its partner whose security is not enough and contagious to others [25]. In cyber insurance, a degree of security interdependence is one of the unique peculiarities [25]. Its impact may vary depending on various factors. Also, its result of a theoretical analysis depends on a chosen security investment model, which is either continuous or discrete. Several researchers [35, 34, 38, 27] come to a similar conclusion that cyber insurance cannot be an incentive to invest in self-protection if discrete investment model is considered. For continuous model, some studies, i.e., H.Ogut et al., and others [35, 50] have shown that the degree of security interdependence has a positive impact on cyber insurers since it discourages an insured to invest in its self-protection but prefer to have an insurance option.

Pal et al., [113] analysed the impact of security interdependence in

both competitive and non-competitive insurance markets with a presence of discrete investment model. The additional instrument was the "fine and rebate" mechanism in their work. The authors highlighted that, with discrimination of contracts, cyber insurance could be an incentive in self-protection. However, to satisfy the result, an insurer should be able to have full knowledge of insureds' security level. Also, Marc Lelarge and Jean Bolot [49] found that the degree of security interdependency has also a positive impact on the incentive of the insured's to invest in its self-protection. It is worth noting that the authors considered an oversimplified discrete security investment model; either to be high or low, in contrast to other literature that assumed continues model, i.e., H.Ogut et al., [35] and G.A.Schwartz et al., [30]. Thus, the question is "what if security interdependence falls between high and low levels?".

In this chapter, we theoretically show how the degree of security interdependence affects the incentive of the insured to invest in self-protection by modelling the competitive insurance market.

5.2.1 Formal Analysis

Table 5.1 defines how the security investment x varies in 4 different cases – when cyber insurance is available and not an option, as well as whether security interdependency is considered. So far, Ehrlich et al., [41] showed

	Insurance available (IA)	No-Insurance available (NA)
No (low) interdependence (LI)	x_{LI}^{IA}	x_{LI}^{NA}
High interdependence (HI)	x_{HI}^{IA}	x_{HI}^{NA}

Table 5.1: Problem statement description

that cyber insurance might be an incentive to invest for self-protection

if there is no/low-security interdependency in place (yet, this completely depends on the initial conditions, i.e., the probability and utility functions applied for modelling): x_{LI}^{IA} *cond* x_{LI}^{NA}. Also, according to the study of Ogut et al., [35], the investments with insurance for independent cases are higher than for cases with a higher degree of interdependence: $x_{LI}^{IA} \geq x_{HI}^{IA}$; and without the insurance case, the following condition holds ($x_{LI}^{NA} \geq x_{HI}^{NA}$). *What we are interested in is to find the security investments level for cases of with and without cyber insurance option when there is a higher degree of security interdependency in place* x_{HI}^{NA} ? x_{HI}^{IA}. *More specifically, we analyse how security interdependence plays for the relation of security investment and cyber insurance.*

Security Interdependence

For the analysis, we use a similar formalisation to the one used by H.Ogut et al., [35], I.Ehlrich and G.S.Becker [41], W.Shim [116], where we use the single threat scenario instead of multiple-threats that we have considered so far.

We assume the probability of attack can be illustrated as $p(x, \Pi)$ simply taking both security investment x and the degree of interdependency $\Pi \in [0, 1]$. It also depends on both direct $\gamma(x)$ and indirect (know as aggregated probability of contagion $(1 - \Pi)$) probability of attack:

$$p(x, \Pi) = 1 - (1 - \gamma(x))\Pi, \tag{5.6}$$

where a direct likelihood solely depends on organisation's security investments while indirect is caused by its partners. Naturally, the direct probability of attack decreases with every increase of security investments ($\gamma' < 0$) and the efficiency of investments decreases ($\gamma'' > 0$). On the other hand, the aggregated probability of contagion $(1 - \Pi_i)$ per organisation i can be computed as it has been mentioned in several works, i.e., [25, 35],

under the condition that the bilateral probabilities of contagion $\mu_{i,j}$ and the investments of other organisations X_{-i} are known:

$$1 - \Pi_i = 1 - \prod_{\forall j \neq i} (1 - \mu_{i,j} * \gamma(x_j)) \tag{5.7}$$

To make the investigation conceptually simpler, we use only Π for the further analyses and it can be ranged between [0,1], where it is obviously independent if $\Pi = 1$.

Now, let us re-write the expected utility of the organisation i without a cyber insurance option as follows:

$$E[U(W)] = U_{NN} * (1 - p(x, \Pi)) + U_{NL} * p(x, \Pi), \ where \tag{5.8}$$

$$U_{NN} = U(W^0 - x) \text{ is the utility if no incident occurs;} \tag{5.9}$$

$$U_{NL} = U(W^0 - L - x) \text{ is the utility if an incident occurs.} \tag{5.10}$$

To find the optimal investment for organisation i, let's take the First Order Condition (FOC) as the following equation:

$$\gamma'(x^N)\Pi = \frac{(1 - (1 - \gamma(x^N))\Pi)U'_{NL} + (1 - \gamma(x^N))\Pi * U'_{NN}}{(U_{NL} - U_{NN}).}. \tag{5.11}$$

However, our goal is to investigate the scenario where cyber insurance option is available. So the expected utility is:

$$E[U(W)] = U_{IN} * (1 - p(x, \Pi)) + U_{IL} * p(x, \Pi); \ where \tag{5.12}$$

$$U_{IN} = U(W^0 - p(x, \Pi) * I - x) \text{ no incident occurs;} \tag{5.13}$$

$$U_{IL} = U(W^0 - L - p(x, \Pi) * I + I - x) \text{ incident occurs.} \tag{5.14}$$

We again take FOC for I as well as for x, following H.Ogut et al., [35] and I.Ehlrich and G.S.Becker [41]. The optimal indemnity I^* is equal to loss L as it is investigated as the following proof:

$$\frac{\partial E[U(W)]}{\partial I} = \frac{\partial((p(x, \Pi) * U_{IL}) + U_{IN}(1 - p(x, \Pi)))}{\partial I} = 0 \tag{5.15}$$

$$(1 - p(x, \Pi)) * p(x, \Pi) * (U'_{IL} - U'_{IN}) = 0. \tag{5.16}$$

In reality, we cannot consider the probability of attack as $p(x) = 1$ or $p(x) = 0$ since such situations do not need to have a cyber insurance option. We, therefore, ignore these situations so that we obtain $U'_{IL} = U'_{IN}$ which leads to the following solution for optimal investments:

$$\gamma'(x^I)\Pi = -\frac{1}{L}. \tag{5.17}$$

If we see Equations 5.11 and 5.17, we can observe some interesting points on x^I and x^N values. For instance, security investments in case of insurance is higher than no insurance available case, $\gamma'(x^I) > \gamma'(x^N)$. Also, in Equations 5.11 and 5.17, it is easy to see that the interdependency Π makes an impact on optimal investments. We, therefore, would like to know if there is such a Π, which makes $\gamma'(x^I) = \gamma'(x^N)$. In other words, we would like to know if the following equation holds:

$$\frac{(1-(1-\gamma(x^N))\Pi)U'_{NL} + (1-\gamma(x^N))\Pi * U'_{NN}}{(U_{NL} - U_{NN})} = -\frac{1}{L}. \tag{5.18}$$

Let us re-write the security interdependency in a simpler way based on Equation 5.11 as following:

$$\begin{aligned} \gamma'(x^N)(U_{NL} - U_{NN})\Pi = \\ = U'_{NL} - (1-\gamma(x^N))\Pi * U'_{NL} + (1-\gamma(x^N))\Pi * U'_{NN} \end{aligned} \tag{5.19}$$

Above-mentioned transformation leads us to the following result:

$$\Pi(\pi'(x^N)(U_{NL} - U_{NN}) + (1-\pi(x^N))(U'_{NL} - U'_{NN})) = U'_{NL} \tag{5.20}$$

After the transformation for defining Π, it becomes easy to investigate a function fn which is defined by the following system[1]:

$$\begin{cases} \Pi = \frac{U'_{NL}}{\gamma'(x)(U_{NL}-U_{NN})+(1-\gamma(x))(U'_{NL}-U'_{NN})}; \\ f = \frac{(1-(1-\gamma(x))\Pi)U'_{NL}+(1-\gamma(x))\Pi * U'_{NN}}{U_{NL}-U_{NN}}. \end{cases} \tag{5.21}$$

[1]Unfortunatelly, it is impossible to write just one equation as $f(\Pi)$, since the first equation in the system cannot be shown in an explicit form $x(\Pi)$.

Now, let's consider binary cases: $\Pi = 1$ and $\Pi = 0$, start with the former case. What is interesting is that security investment in case of insurance is lower than in case of no-insurance available. ($x_{LI}^{IA} = x^{I_1} < x^{N_1} = x_{LI}^{NA}$):

$$\frac{\gamma(x^{N_1})U'_{NL}(x^{N_1}) + (1-\gamma(x^{N_1}))U'_{NN}(x^{N_1})}{(U_{NL}(x^{N_1}) - U_{NN}(x^{N_1}))} > -\frac{1}{L}. \tag{5.22}$$

Here, we simply refer x^{I_1} or x^{N_1} as investments with or without insurance, respectively when security interdependence degree is equal to 1 (or first case). Then, considering $\Pi = 0$ or the second case (x^{N_2}), we see, that:

$$\frac{U'_{NL}(x^{N_2})}{(U_{NL}(x^{N_2}) - U_{NN}(x^{N_2}))} < -\frac{1}{L}, \tag{5.23}$$

since for a concave function $U'_{NL} * L > U_{NN} - U_{NL}$. Since function $f(\Pi)$ is continuous, then according to the Intermediate Value Theorem, there is such $1 > \bar{\Pi} > 0$ which makes $f(\bar{\Pi}) = -\frac{1}{L}$ and Equation 5.18 holds for this $\bar{\Pi}$ ($x_{HI}^{NA} = x_{HI}^{IA}$).

It is worth mentioning that very low values of security interdependency may require negative investments which are not possible. Thus, it is more meaningful to assume the minimal reasonable value of security investments, the minimal value of $\gamma'(x^N = 0)$ and $x^N = 0$ instead of the case with $\Pi = 0$. If $\gamma'(x^N = 0) < -1/L$ condition holds, it can be concluded that the required value $\bar{\Pi}$ is between 1 and the $\bar{\Pi}$ value found from the first equation of (Equation System 5.21) for $x^N = 0$.

5.2.2 Summary of the section

In this section, we have theoretically investigated the effect of security interdependence on security investments by considering both with and without having a cyber insurance option. As a result, we found that, with a certain degree of security interdependence, cyber insurance encourages the organisations to invest for self-protection equally to (and even more in comparison

with) the scenario of no insurance option is available. The aforementioned conclusion is true if we consider that security investments are higher in case of no insurance option available without the degree of security interdependence. In other words, we may conclude that the security interdependence could be a positive factor that not only affected cyber insurance but also could elevate the security investments. It is worth highlighting that the analysis we have provided is just at the initial phase and more investigations should be done in future. For instance, we have not shown how much security investments increase or drop and did not compare the situation with an independent cyber insurance case. Also, the information asymmetry problem has not been considered. Having an information asymmetry problem in the model considerably changes the security investments of an insured as well as other's incentive to invest. Even though having some assumptions, we believe that the initial result already leads us to further directions.

Chapter 6

Prevention of security investment drop in Non-Competitive Insurance Market

6.1 Introduction

In this chapter, we analyse the relationship between cyber insurance and security investments in a non-competitive insurance market model. As we introduced in Chapter 3, a competitive insurance market is considered as a generic model and widely used in theoretical investigations because of its simplicity [25, 94, 95]. On the other hand, the non-competitive insurance market makes the analysis more difficult and theoretically complex to solve. The reason is that the premium in this market is computed in a different way than it is in the competitive insurance market. Usually, it adds an additional loading factor (i.e., administrative cost) for the premium. In particular, it makes the optimisation of security investments complex and affects the behaviour of insureds to decide on their security investments.

Some researchers [35, 38, 34] underline that the incentive of investing for self-protection decreases when an insured has a cyber insurance option. Similar to the one of Ogut et al., [35] works, we conduct the analyse

considering continues security investment model and use a generic class of utility functions for modelling insureds' satisfaction. We further conceptually model a single-threat case and leave the multi-threats case for future analysis if the result is satisfying in this investigation.

The chapter is structured as follows. Section 6.2 underlines the problem to solve in two cases: with cyber insurance available and without it. The following, Section 6.3, introduces the proposed solution and describes how security investments can be raised with a raise of premium. Also, we have to investigate the effect of security interdependence in Section 6.4. Then, Section 6.5 validates the theoretical contribution considering two specific examples. Section 6.6 summarises the chapter and achievements.

6.2 Basic Formalization

In previous chapters, we have only considered a competitive insurance market without a loading factor for premium estimation. In a non-competitive insurance market, the premium is computed:

$$P = (1 + \lambda) \times Risk = (1 + \lambda) * p * (x)I \tag{6.1}$$

where, the λ is a loading factor. If $\lambda = 0$, one can say that the market is competitive, otherwise it is a non-competitive market model. Thus our expected utility will be:

$$E[U(W)] = U_{IN} * (1 - p(x)) + U_{IL} * p(x);\ where \tag{6.2}$$

$$U_{IN} = U(W^0 - (1 + \lambda) * p(x)I - x) \text{ no incident occurs;} \tag{6.3}$$

$$U_{IL} = U(W^0 - L - (1 + \lambda) * p(x)I + I - x) \text{ incident occurs.} \tag{6.4}$$

In the case of the competitive insurance market where $\lambda = 0$, it is possible to find the optimal investment, which is equal to[1]:

$$x^I = -\frac{1}{L}. \tag{6.5}$$

According to some researchers, security investments with cyber insurance option is higher or at least equal to security investments without cyber insurance case, formally:

$$p'(x^N) \leq p'(x^I) \quad or \quad p'(x^N) \leq -\frac{1}{L}. \tag{6.6}$$

However, some [35, 38, 34] claim that cyber insurance discourages investing for the self-protection:

$$p'(x^N) \geq -\frac{1}{L}. \tag{6.7}$$

Now, the interesting question is that, *"Is it possible to raise the security investments to the level of no insurance case by optimising the loading factor?"*. Moreover, we would like to investigate the incentive of an organisation buying cyber insurance regardless of the increased price.

6.3 Raising Security Investment Level

We first consider the situation where we have only security investments option without a cyber insurance alternative. Let's define the utilities as follows:

$$U_{NN} = U(W^0 - x) \text{ if no incident occurs;} \tag{6.8}$$

$$U_{NL} = U(W^0 - L - x) \text{ if an incident occurs.} \tag{6.9}$$

Thus, the expected utility in this case is:

$$E[U(W)] = p(x^N)U_{NL} + (1 - p(x^N))U_{NN}. \tag{6.10}$$

[1]See the proof in [35] or [41] for a single threat scenario, and also our proposed solution in the previous chapter considering multiple-threats.

To find the optimal security investment, we take the First Oder Condition (FOC) for x^N

$$\frac{\partial E[U(W)]}{\partial x} =$$
$$p'(x^N)U_{NL} - p(x^N)U'_{NL} - (1-p(x^N))U'_{NN} - p'(x^N)U_{NN} = 0; \quad (6.11)$$
$$p'(x^N)(U_{NL} - U_{NN}) = p(x^N) * U'_{NL} + (1-px^N)U'_{NN}; \quad (6.12)$$
$$p'(x^N) = \frac{p(x^N) * U'_{NL} + (1-p(x^N))U'_{NN}}{(U_{NL} - U_{NN})}. \quad (6.13)$$

The solution to Equation 6.13 will provide us with the optimal security investments an insured should invest in case of no cyber insurance case.

Let us conduct the same investigation that we have done for competitive insurance market analysis. In order to find the optimal investments x^* and indemnity I^*, we take FOC for Equation 6.4.

$$\frac{\partial E[U(W)]}{\partial I} =$$
$$p(x) * U'_{IL}(1 - p(x)(1+\lambda)) - (1-p(x))(1+\lambda)p(x)U'_{IN} = 0. \quad (6.14)$$

From Equation 6.14, it is transformed into:

$$\frac{U'_{IL}}{U'_{IN}} = \frac{(1-p(x))(1+\lambda)}{1-p(x)(1+\lambda)} \; or \quad (6.15)$$

$$1 + \lambda = \frac{U'_{IL}}{U'_{IN}(1-p(x)) + p(x)U'_{IL}}. \quad (6.16)$$

Also, for the security investment, we do the same analysis:

$$\frac{\partial E[U(W)]}{\partial x} = p'(x^*) * U_{IL} - p(x^*) * U'_{IL}(p' * (x^*)(1+\lambda)I + 1) -$$
$$(1-p(x^*))U'_{IN}(p'(x^*)(1+\lambda)I + 1) - p'(x^*)U_{IN} = 0 \quad (6.17)$$

After some simple transformations, the above-mentioned equation forms:

$$\frac{U_{IL} - U_{IN}}{(p(x^*)U'_{IL} + (1-p(x^*))U'_{IN})} - \frac{1}{p'(x^*)} = (1+\lambda)I \quad (6.18)$$

As we described before, the goal is to ensure that the security investments when cyber insurance is available reach the level of investments without the insurance case, i.e., $x^* = x^N$. At the same time, the amount of indemnity should be optimal $I = I^*$. To solve the problem (λ, I^*), the following system of equations should be solved:

$$\begin{cases} 1 + \lambda = \frac{U'_{IL}}{U'_{IN}(1-p(x^*))+p(x^*)U'_{IL}}; \\ \frac{(U_{IL}-U_{IN})}{(p(x^*)U'_{IL}+(1-p(x^*))U'_{IN})} - \frac{1}{p'(x^*)} = (1+\lambda)I^*. \end{cases} \tag{6.19}$$

Even though the system is hard to solve, the answer can be found (see Section 6.5) when all functions and variables are precisely defined. The main question is to find whether the system has a solution for indemnity which is greater than 0, i.e., $I^* > 0$ if (λ, I^*) is the solution for Equation 6.19.

Theorem 1 *When the utility function is a decreasing absolute risk aversion (DARA) type and the security investments for the competitive insurance market model is lower than in case of no insurance scenario, it is possible to find such a setting of λ for the non-competitive cyber insurance market model which ensures that:*

1. *the security investments level can reach the level of investments without cyber insurance case ($x^* = x^N$).*
2. *Indemnity is a non-zero value ($I^* > 0$)*

Proof First, let's put Equation 6.16 to Equation 6.18:

$$\frac{(U_{IL} - U_{IN})}{(p(x^*)U'_{IL} + (1-p(x^*))U'_{IN})} - \frac{1}{p'(x^*)} = \frac{U'_{IL}}{U'_{IN}(1-p(x)) + p(x)} I; \tag{6.20}$$

$$-\frac{1}{p'(x^*)} + \frac{(U_{IL} - U_{IN} - I * U'_{IL})}{(p(x*)U'_{IL} + (1-p(x^*))U'_{IN})} = f(I^*) = 0. \tag{6.21}$$

It is easy to observe that if an organisation does not have an insurance option ($I^* = 0$), the optimal investment is equal to the level when there is

no cyber insurance available. In this regard, we would like to investigate $f(I^*)$ considering whether there is another solution for Equation 6.21 on the interval $I^* \in [0, L]$

Moreover, when the indemnity is equal to the loss (i.e., full insurance case $I^* = L$), it can be seen that, from Equations 6.4, $U_{IL} = U_{IN}$ and the right summand of $f(I^*)$ is equal to $-L$. If we take into account the assumption from Equation 6.7, we see that:

$$\frac{1}{p'(x^*)} = \frac{1}{p'(x^N)} < -L. \tag{6.22}$$

Basically, from Equation 6.22, it can be concluded that $f(I^*)|_{I^*=L} > 0$. However, this solution, $I = L$, is not the absolute solution which can describe the behaviour of $f(I^*)$ function.

We have found that $f'(I^*)|_{I^*=0} < 0$ (see the proof in below):

Proof: We first take the derivative by indemnity I as follows:

$$\begin{aligned}
&\frac{df}{dI^*} = \\
&\frac{\left[(1-(1+\lambda)p(x^*) - p(x^*)I\frac{d\lambda}{dI^*})U'_{IL} - U'_{IL}\right]\left[p(x^*)U'_{IL} + (1-p(x^*))U'_{IN}\right]}{(p(x^*))U'_{IL} + (1-p(x^*))U'_{IN})^2} + \\
&\frac{\left[(1+\lambda)p(x^*) + p(x^*)I\frac{d\lambda}{dI^*})\right]U'_{IN}\left[p(x^*)U'_{IL} + (1-p(x^*))U'_{IN}\right]}{((p(x^*))U'_{IL} + (1-p(x^*))U'_{IN})^2} - \\
&\frac{I^*\left[1-(1+\lambda)p(x^*) - p(x^*)I\frac{d\lambda}{dI^*}\right]U''_{IL}\left[p(x^*)U'_{IL} + (1-p(x^*)U'_{IN}\right]}{((p(x^*))U'_{IL} + (1-p(x^*))U'_{IN})^2} - \\
&\frac{\left[U_{IL} - U_{IN} - I^*U'_{IL}\right]p(x^*)\left[1-(1+\lambda)p(x^*) - p(x^*)I\frac{d\lambda}{dI^*}\right]U''_{IL}}{(p(x^*))U'_{IL} + (1-p(x^*))U'_{IN})^2} - \\
&\frac{\left[U_{IL} - U_{IN} - I^*U'_{IL}\right]p(x^*)(1-p(x^*))\left[-(1+\lambda)p(x^*) - p(x^*)I\frac{d\lambda}{dI^*}\right]U''_{IN}}{((p(x^*))U'_{IL} + (1-p(x^*))U'_{IN})^2}.
\end{aligned} \tag{6.23}$$

From the first derivative, we would like to know its sign when $I^* = 0$. It is evident that we should only focus on dividend since the divisor is positive

because of the square operation. Then, $U'_{IL}|_{I^*=0} = U'_{NL}$ and $U'_{NN}|_{I^*=0} = U'_{NN}$ because if there is no indemnity it can be considered as a case without insurance. We are able to reduce the first part of Equation 6.23 by U'_{IL} inside the first brackets. Also, the third part is equal to 0 as well as all sub-parts with $\frac{d\lambda}{dI^*}$. If we move out $p(x^*)(1-(1+\lambda)p(x^*))$ in the third part, we get:

$$\begin{aligned}
&(1+\lambda)p(x^*)(-U'_{NL}+U'_{NN})(p(x^*)U'_{NL}+(1-p(x^*))U'_{NN})+\\
&(U_{NN}-U_{NL})p(x^*)(1-(1+\lambda)p(x^*))[(U''_{NL}-\frac{(1-p(x^*))(1+\lambda)}{(1-(1+\lambda)p(x^*))}U''_{NN})]=\\
&(1+\lambda)p(x^*)(-U'_{NL}+U'_{NN})(p(x^*)U'_{NL}+(1-p(x^*))U'_{NN})+\\
&(U_{NN}-U_{NL})p(x^*)(1-(1+\lambda)p(x^*))[(U''_{NL}U'_{NN}-U''_{NN}U'_{NL})]\frac{1}{U'_{NN}}.
\end{aligned} \tag{6.24}$$

Since we know that $U'_{NL} > U'_{NN}$ and the first derivative is greater than 0, the first summand is negative as well as $U_{NN} > U_{NL}$ where the utility function is always positive. Moreover, $1 > (1+\lambda)p(x^*)$, otherwise an insured should pay more than it recovers from the loss. Now, the only part we should consider is $(U''_{NL}U'_{NN} - U''_{NN}U'_{NL})$.

We recall the definition of *coefficient of absolute risk aversion* for the utility functions as:

$$A(W) = -\frac{U''(\mathbf{W})}{U'(\mathbf{W})}. \tag{6.25}$$

Taking into consideration of practical examples of decreasing absolute risk aversion (DARA) functions, to avoid complexities, we assume non-increasing risk aversion (CARA and DARA):

$$\frac{\partial A(\mathbf{W})}{\partial \mathbf{W}} \leq 0. \tag{6.26}$$

In other words $A(W_{NL}) \geq A(W_{NN})$, where W_{NL} is the final wealth when

there is an incident, while W_{NN} is the financial position of an insured without any incidents.

Thus, $(U''_{NL}U_{NN} - U''_{NN}U'_{NL}) = U''_{NN}U'_{NL}[A(W_{NN}) - A(W_{NL})] \leq 0$ and the second summand in the overall formula is negative or zero.

End of Proof

□

Since the function is continuous (on the interval $I^* \in [0; L]$[2]) and $f(I^*)|_{I^*=L} > 0$, there must be at least one point, according to the Intermediate Value Theorem, with $I^* > 0$ which is the solution to Equation 6.21 (the point, where function $f(I^*) = 0$ for $I^* \in (0; L)$).

Insureds prefer to buy insurance. For solving the problem, we have two different solutions to use as is shown above: $I^* = 0$ and $I^* > 0$.

From the perspective of an insured, it is clear that the insured selects the best solution which maximises its expected utility $E[U(W)]$ and has always the option "not having cyber insurance". On the other hand, insurers would like to set the optimal λ to ensure that the insured wants to have the insurance option. To find whether having an insurance case can be better-off, we compare the cases:

$$\begin{aligned} &E[U(W)]|_{I^*\neq 0} - E[U(W)]|_{I^*=0} = \\ &p(x^N)U_{IL} + (1 - p(x^N))U_{IN} - p(x^N)U_{NL} - (1 - p(x^N))U_{NN} = \\ &p(x^N)(U_{IL} - U_{NL}) + (1 - p(x^N))(U_{NN} - U_{IN}). \end{aligned} \tag{6.27}$$

Now, let's recall that $U_{IL} \geq U_{NL}$ and $U_{NN} \geq U_{IN}$, while the utility function is convex, i.e., $U_{IL} - U_{NL} < U'_{IL}(I^*(1 - p(x^N)(1 + \lambda)))$ and $U_{NN} - U_{IN} > U'_{IN}(I * p(x^N)(1 + \lambda))$. Finally, using Equation 6.15, it is possible find that

[2] $f'(I^*)$ is continuous on the interval $I^* \in [0; L]$ since neither $p'(x^*) = 0$ nor $p(x^*)U'_{IL} + (1 - p(x^*))U'_{IN}) = 0$ for realistic values.

the result is greater than 0.

$$E[U(W)]|_{I^*\neq 0} - E[U(W)]|_{I^*=0} \geq$$
$$p(x^N)U'_{IL}(I^*(1-p(x^N)(1+\lambda))) - (1-p(x^N))U'_{IN}(I^*p(x^N)(1+\lambda)) = 0. \tag{6.28}$$

So after the comparison, for any $(I * E[U(W)]|_{I^*\neq 0} \geq E[U(W)]|_{I^*=0})$, we have come to a conclusion that an insured always prefers to buy some insurance if the settings are as defined by solution of Equation 6.19.

Moreover, it is easy to see that if $\lambda = 0$, then $I^* = L$. Now, if $I^* = 0$, then

$$\lambda = \frac{(U'_{NL} - U'_{NN})(1-p(x))}{(U'_{NL} - U'_{NN})p(x) + U'_{NN}}. \tag{6.29}$$

As a result of Equation 6.29, we can conclude that the loading factor forces the security level to be equal to x^N which belongs to the interval $[0, \frac{(U'_{NL}-U'_{NN})(1-p(x))}{(U'_{NL}-U'_{NN})p(x)+U'_{NN}}]$.

Using Equation 6.15 for $I \neq 0$ and $I = 0$, it is easy to find that the loading factor in the first case that is always lower:

$$\frac{(1-p(x))}{p(x) + \frac{1}{\frac{U'_{NL}}{U'_{NN}}-1}} \geq \frac{(1-p(x))}{p(x) + \frac{1}{\frac{U'_{IL}}{U'_{IN}}-1}}, \quad since\ U'_{NL} \geq U'_{NN}\ and\ U'_{IL} \leq U'_{IN}. \tag{6.30}$$

6.4 Interdependence of security.

So far, we have investigated the independent case, where the likelihood of an attack is only considered as the direct probability of attack to the organisation. In reality, there is always interconnectedness of systems/networks, and we, therefore, consider a degree of security interdependency for the analysis. As we described previously (Equation 5.6 in Chapter 5.2), the

probability of attack will be computed with the presence of interdependence degree.

$$p_i(x_i X_{-i}) = 1 - (1 - \gamma_i(x_i)) \cdot \Pi_{-i} \quad \text{, where}$$
$$\Pi_{-i} = \prod_{\forall j \neq i} (1 - \mu \cdot \gamma_j x_j). \tag{6.31}$$

In this analysis, we do not intend to model the whole network and instead we focus on a single insured. Thus, we can omit some indexes i and $-i$ and skip X_{-i} to make the analysis understandable.

However, in this analysis, the security interdependency does not much impact the investigation of finding I and λ. Thus, we simply should use Equation 6.31 instead of simple p_i.

$$\begin{cases} 1 + \lambda = \frac{U'_{IL}}{U'_{IN}((1-\gamma(x^*))*\Pi)+(\gamma(x^*)*\Pi)U'_{IL}}; \\ \frac{(U_{IL}-U_{IN})}{U'_{IN}((1-\gamma(x^*))*\Pi)+(\gamma(x^*)*\Pi)U'_{IL}} - \frac{1}{\gamma(x^*)*\Pi} = (1+\lambda)I^*. \end{cases} \tag{6.32}$$

6.5 Use Case Examples

In this section, we would like to validate the current theoretical solution by using two well-known DARA utility functions which are frequently used in cyber insurance [25] literature: Constant Absolute Risk Aversion (CARA) and Constant Relevant Risk Aversion (CRRA) functions. It is worth mentioning that CARA and CRRA utility functions are only useful examples, while the findings from Section 6.3 are valid for any concave utility functions.

6.5.1 CARA utility function

The main requirement for Constant Absolute Risk Aversion (CARA) function is the following:

$$-\frac{U''(W)}{U'(W)} = \sigma; \quad \sigma > 0. \tag{6.33}$$

To satisfy this relation, the following exponential function is denoted:

$$U(W) = 1 - \exp^{-\sigma W}; \quad U'(W) = \sigma \exp^{-\sigma W}; \quad U"(W) = -\sigma^2 \exp^{-\sigma W}. \tag{6.34}$$

Now, let's recall the Equation system 6.19 and apply the above function so that the following result comes with using the first equation:

$$e^{\sigma(L-I^*)} = \frac{(1+\lambda)(1-p(x^*))}{(1-p(x^*)(1+\lambda))} \quad or \tag{6.35}$$

$$I^* = L - \frac{1}{\sigma} ln \left[\frac{(1+\lambda)(1-p(x^*))}{(1-p(x^*)(1+\lambda))} \right]. \tag{6.36}$$

Also, the second equation from the system is turned into:

$$\frac{1}{\sigma} \frac{1 - e^{\sigma(L-I^*)}}{1 - p(x^*) + p(x^*)(e^{\sigma(L-I^*)})} - \frac{1}{p'(x^*)} = (1+\lambda) I^* \quad or \tag{6.37}$$

$$\frac{1}{\sigma} \frac{\lambda}{1-p(x^*)} - \frac{1}{p'(x^*)} = (1+\lambda) I^*. \tag{6.38}$$

The following form is assumed for $f(I^*)$ function from Equation 6.21:

$$\frac{1}{\sigma} \frac{\lambda}{1-p(x^*)} - \frac{1}{p(x^*)} - (1+\lambda) I^* = f(I^*). \tag{6.39}$$

Now, it can be seen that the loading factor (λ) is the solution of the following transformed equation:

$$\frac{1}{\sigma(1+\lambda)} \frac{\lambda}{1-p(x^*)} - \frac{1}{p'(x^*)(1+\lambda)} = L - \frac{1}{\sigma} ln \left[\frac{(1+\lambda)(1-p(x^*))}{(1-p(x^*)(1+\lambda))} \right]. \tag{6.40}$$

Although the above equation is theoretically challenging to solve, the solution can be found with applying graphic solutions or approximation algorithms.

6.5.2 CRRA utility function

The main condition to hold for Constant Relative Risk Aversion (CRRA) utility function is the following relation:

$$-\frac{U''(W)}{U'(W)} = \frac{\sigma}{W}; \quad \sigma > 0. \tag{6.41}$$

Thus, the utility function can de described as follows:

$$U(W) = \begin{cases} \frac{W^{1-\sigma}}{1-\sigma} & \text{for } \sigma \neq 1 \\ log(W) & \text{for } \sigma = 1 \end{cases}; \quad U'W = W^{-\sigma}; \quad U''W = -\sigma\frac{W^{-\sigma}}{W}. \tag{6.42}$$

If there is no loss of generality, we assume that $\sigma \neq 1$. Thus, the same as CARA function, let us apply this utility function to the Equation system 6.19 so that the following can be achieved using the first equation:

$$\left(\frac{W^0 - p(x^*)(1+\lambda)I^* - x^*}{W^0 - L + I - p(x^*)(1+\lambda)I^* - x^*}\right)^\sigma = \frac{(1+\lambda)(1-p(x^*))}{(1-p(x^*)(1+\lambda))} = \alpha \quad or \tag{6.43}$$

$$I^* = \frac{L\sqrt[\sigma]{\alpha} - (W^0 - x^*)(\sqrt[\sigma]{\alpha} - 1)}{\sqrt[\sigma]{\alpha} - p(x^*)(1+\lambda)(\sqrt[\sigma]{\alpha} - 1)}. \tag{6.44}$$

And, the second equation from the system is transformed into:

$$\frac{1}{1-\sigma}\frac{(W^0 - p(x^*)(1+\lambda)I^* - x^*)(\alpha-1) - \alpha L + \alpha I^*}{p(x^*)\alpha + (1-p(x^*))} - \frac{1}{p(x^*)} = (1+\lambda)I^*;$$

$$I^* = \frac{p(x^*)((W^* - x^*)(\alpha-1) - \alpha L) - \beta}{p(x^*)((1+\lambda)\beta + p(x^*)(1+\lambda)(\alpha-1) - \alpha)}, \tag{6.45}$$

where $\beta = (1-\sigma)(p(x^*)\alpha + (1-p(x^*)))$.

$f(I^*)$ function from Equation 6.21 considers the following form:

$$f(I^*) = \frac{(W^0 - p(x^*)(1+\lambda)I^* - x^*)(\alpha-1) - \alpha L + \alpha I^*}{(1-\sigma)(p(x^*)\alpha + (1-p(x^*)))} - \frac{1}{p(x^*)} - (1+\lambda)I^*. \tag{6.46}$$

Now, it can be seen that the loading factor (λ) is the solution of the following transformed equation:

$$\frac{L-(W^0-x^*)(\sqrt[\sigma]{\alpha}-1)}{\sqrt[\sigma]{\alpha}-p(x^*)(1+\lambda)(\sqrt[\sigma]{\alpha}-1)}=\frac{p(x^*)((W^0-x^*)(\alpha-1)-\alpha L)-\beta}{p(x^*)(1+\lambda)\beta+p(x^*)(1+\lambda)(\alpha-1)-\alpha}. \tag{6.47}$$

Although the Equation 6.47 is theoretically hard to solve, the solution can be found with applying graphic solutions or approximation algorithms.

6.5.3 Numerical analysis

To show whether the theoretical solution is correct, we would like to illustrate the validation with a couple of numerical analyses. We set the initial wealth at 20 (thousand) euro and the loss at 10 (thousand) euro. Also, we use the same $\sigma = 0.1$ for both CARA and CRRA utility functions. The probability of functions is defined as follows (ensuring that $p'(x^*) < 0$ and $p''(x^*) < 0$):

$$p(x^*)=\frac{0.2}{(1+x)}. \tag{6.48}$$

Assuming these constant settings, We can find both λ and I.

CARA Let's start with CARA utility function with $\sigma = 0.1$. To obtain x^N, which is the target to find when cyber insurance is available case $x^N = x^*$, we first solve Equation 6.13. With defined probability function (Equation 6.48), Equation 6.13 can be seen as a quadratic equation where one solution is always negative. The second solution for the case is $x^N \approx 0.69$. As is shown, the probability of attack we compute satisfies the condition stated in Equation 6.7 $p'(x^N) \approx -0.07 > -1/10 = -0.1$.

In Figure 6.1, the left parts shows the behaviour (see Equation 6.39) of auxiliary function $f(I^*)$. Based on the reasoning in Section 6.3, when

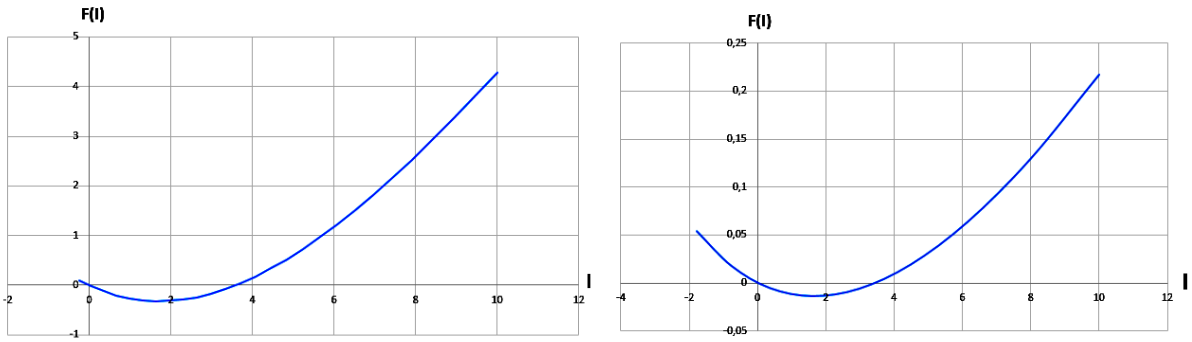


Figure 6.1: $f(I)$ for CARA and CRRA examples.

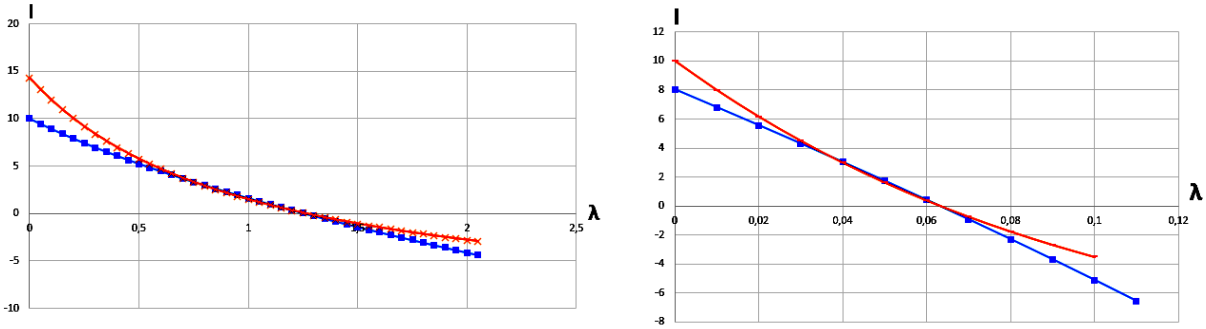


Figure 6.2: Intersections of $I(\lambda)$ for Equations 6.40(left) and 6.47 (right).

$I^* = 0$ and $\lambda \approx 1.26$, there is an intersection of the function and line $f(I^*) = 0$. Moreover, there is also at least one more intersection with this line for $I^* \approx 3,5946 \neq 0$ and $\lambda \approx 0.7153$.

Naturally, instead of considering the auxiliary function for finding the optimal values, it is more applicable to take into account Equation 6.40 and find the intersection points of the left and right parts of the equation. These functions are depicted in the left part of Figure 6.2. We have derived a simple hybrid root-finding algorithm[3] to find the resulting values of I^* and λ.

[3]The considered interval is first cut into small pieces and assign border values of different signs for the pieces. Then, the bisection method is used for halving the pieces to check the signs of the function on border values. It always leaves the half with different signs of the function on the border until the last half is shorter than the allowed error.

CRRA As we have done for CARA, the same analysis is applied to CRRA utility function with the exact same $\sigma = 0.1$. Security investments level was found at $x^N \approx 0.43$, which further meets the condition in Equation 6.7 $p'(x^*) \approx -0,0978 > -1/10 = -0.1$.

In the right part of Figure 6.1, it shows the result of $f(I^*)$ using Equation 6.46 and intersection of left and right hand parts of Equation 6.47. The function further intersects the line $f(I^*) = 0$, when $I^* = 0$ and $\lambda \approx 0.063$, plus, there is a cross for $I^* \approx 3.4586 \neq 0$ when $\lambda \approx 0.0267$.

Effect of Interdependency. The final consideration for the numerical analysis is the impact of security interdependency (Π from Equation 6.31) on the incentive of having a cyber insurance option. Three different coefficients are taken for the degree: $\Pi = 1$, $\Pi = 0.9$, and $\Pi = 0.8$, and the result is shown in Figure 6.3.

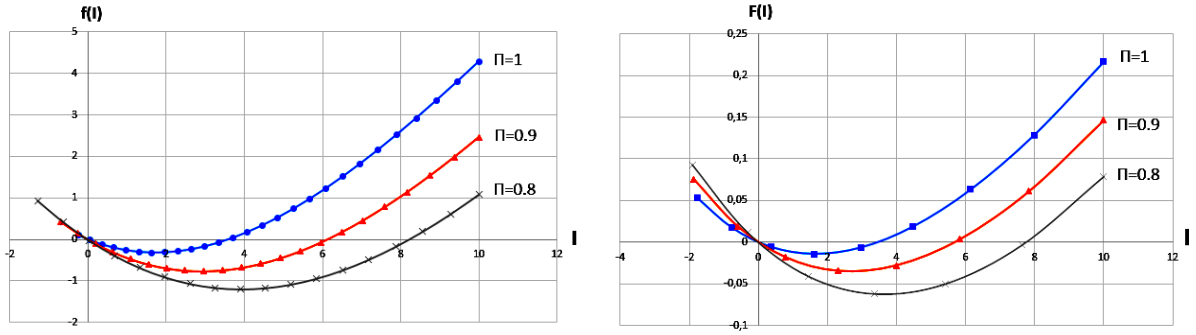


Figure 6.3: $f(I)$ for CARA (left) and CRRA (right) examples with different degree of interdependency.

6.5.4 Discussion

As it is illustrated in the graph, the organisation/insured is more attracted to buying cyber insurance when the point where $f(I)$ line crosses axis I (i.e., $f(I) = 0$) shifts to the left. Thus, it can be concluded that if a

degree of security interdependence increases, the security investment falls but the willingness to have cyber insurance increases. Furthermore, there is the required increase in the insurance cost (i.e., λ) is lower: for CARA $\lambda = 0.1131$ and for CRRA $\lambda = 0.00947$ if $\Pi = 0.8$ vs. for CARA $\lambda = 0.7153$ and for CRRA $\lambda = 0.0267$ if $\Pi = 1$.

It is also clear that function goes lower with the higher degree of interdependency, and, eventually, its right end gets below 0. This indicates that the optimal investments in the presence of cyber insurance with a fair price become higher than the optimal investments with the absence of cyber insurance.

6.6 Summary of the chapter

In this chapter, we have theoretically investigated the possibility of raising the security investments when a cyber insurance option is available, up to the level of no insurance available case. The analysis has shown that, even though the premium is higher, the security investments level can be raised at an equal level as in the no-insurance case by adjusting the loading factor as an incentive. This indicates that the insureds are interested in having at least some portions of cyber insurance option as a treatment alternative. It is worth mentioning that our work has fewer assumptions than the current works have, i.e., [35].

To validate our theoretical analysis, we have applied two generic functions (CARA and CRRA) example for some numerical experiments. Also, with a presence of security interdependence, the result shows that the insureds are more encouraged to buy cyber insurance. Although the increase of security interdependence degree directs the drop of security investments, the insureds are comparably more incentivised by cyber insurance than in the case of a no-insurance case. The effect of security interdependence has

not been completed and we left a thorough analysis for future investigations.

We see a possible direction to continue analysing the possibility of adjusting the insurance price to affect the security investment based on our proposed model. This includes the potential analysis of raising security investments even higher than the no-insurance case. Also, our analysis can be extended with having an information asymmetry issue, i.e., where moral hazard and adverse selection problems have a place. In this regard, contract discrimination ideas could be another incentive when the information asymmetry problem lies. The work by Pal et al., [113] can be integrated for a better understanding of how our analysis can be extended with a fine and rebate mechanism.

Chapter 7

Conclusion of the thesis

In this thesis work, we have analysed the relation between cyber insurance and security investments under various scenarios. In particular, we showed how cyber insurance can be a part of security treatment options through incorporation with security controls. The proposed solution models multiple threats and provide both theoretical and algorithmic approaches to solve the problem. Furthermore, we investigated the possibility of raising the security investments in a non-competitive insurance market model and the effect of security interdependence.

The following sections comprise the main achievements which significantly contribute to the maturity of cyber insurance.

7.1 Competitive Insurance Market

Our first achievement was to theoretically show the potential trade-off between the cyber insurance premium and security investments in a competitive insurance market. The core was to investigate the relationship when there are multiple-threats considered as opposed to current approaches which model a single threat in cyber insurance. We mathematically showed that the indemnity is equal to the loss considering the multiple-threats scenario.

Not only did we mathematically solve the problem, but we also introduced algorithmic solutions for optimising the security control selection process. From the optimisation standpoint, we introduced an innovative version of multiple 0-1 knapsack problem by proposing both exact algorithms (i.e., Dynamic programming and Projection idea) and approximate algorithms (Greedy and Genetic algorithm). What is new in our solution is that we derived the legacy way of solving the knapsack problem and adapted it to our selection problem. The main difference is that our solution finds the optimal budget as an output while the traditional methods look for the best controls within the pre-specified budget.

Based on the use cases, we showed and recommended which method is suitable for which scenario. More importantly, we integrated the proposed solution into an online risk assessment tool that we developed. So, a wider audience had the potential to use our approach.

In summary, our proposed solution investigated one of the biggest challenges in cyber insurance and solved the problem in a way in which an organisation makes a rational decision on its security expenditure.

Future Work. In this work, we have not considered the correlation of security controls' cost which can be addressed in our further analysis. In this regard, the core of the proposed algorithms will be changed according to the extension of our theoretical investigation. Moreover, we will investigate the effect of security interdependence to see how our optimisation solution and the behaviour of the organisation on investing in self-protection will be varied.

7.1.1 Time-to-Compromise metric

Our another contribution in the competitive insurance market was to adapt the time-to-compromise metric to define the security controls' capability

of decreasing the vulnerability. We showed how the metric plays an important role and can be integrated into cyber insurance models. The result initially appeared to be promising in a way that connects the probability of successful attack and vulnerabilities of the system. Last but not least, we see a possible direction on investigating how the time-to-compromise metric can alter the duration of cyber insurance policy (usually a year) depending on organisations' level of security as this has already been done in other insurance areas [51].

7.2 Non-competitive Insurance Market

As opposed to the competitive insurance market, a non-competitive market model is considered much complex and it often requires a rigorous theoretical investigation. In this work, we analysed the problem and theoretically investigated if there is a potential to avoid the drop of security investments when a cyber insurance option is available as a risk treatment alternative. We mathematically showed that the security investments can be raised to the level of no insurance case by optimising the loading factor. Results were numerically validated considering two generic utility functions, CARA and CRRA, to show how they could be applied into a practical scenario.

Future Work. As we modelled the multiple-threats case in a competitive insurance market model our further investigation will be analysing the problem in a non-competitive insurance market. We admit that the theoretical part will require complex analysis, yet once this part will be done, the algorithmic solution will be improved with less complexity. Moreover, in this work, we showed that security investments may potentially be higher than the level without no insurance is the available scenario. Thus, we will conduct a thorough analysis to know whether it could meet our expectation

or not.

7.3 Effect of Security Interdependence

Another contribution of the thesis is that we investigated the effect of security interdependence in both market models. In a competitive insurance market model, we found that cyber insurance can be an incentive for the organisation to invest in self-protection with a certain degree of security interdependence. We also showed that the security interdependence positively affects cyber insurance and it could further elevate the security investments up to a certain level if, initially, the security investments without cyber insurance are higher than the level with cyber insurance case is available.

For the non-competitive insurance market, we have seen some drop-in security investments due to the increase of security interdependence in comparison with the level when there is no cyber insurance option available. We would like to analyse if certain enforcements may encourage the insured to invest more even though the security interdependence increases.

Chapter 8

Appendix

8.1 Notations used in the thesis:

$U()$ $\rightarrow$ Utility function

$E[U()]$ $\rightarrow$ Expected utility function

W^0 $\rightarrow$ Initial wealth

W $\rightarrow$ Final wealth

$\vec{\pi}$ $\rightarrow$ Probability of a threat *survival*

$\vec{F}$ $\rightarrow$ Expected number of threat *attempts*

x $\rightarrow$ Security investment

Π $\rightarrow$ Security interdependency degree

c $\rightarrow$ Cost of a countermeasure

p or $\vec{p}$ $\rightarrow$ Probability of a threat *occurrance*

P $\rightarrow$ Premium

$\vec{z}$ $\rightarrow$ *Number* of threat occurrences

K $\rightarrow$ A set of *available* countermeasures

L or $\vec{L}$ $\rightarrow$ Loss

K_s $\rightarrow$ A set of *selected* countermeasures

I or $\vec{I}$ $\rightarrow$ Indemnity

V $\rightarrow$ A set of vulnerabilities

t $\rightarrow$ Time-to-compromise metric

$\lambda \rightarrow$ Loading factor

$\gamma(x) \rightarrow$ Direct probability of attack

$\mu_{i,j} \rightarrow$ Bilateral probabilities of contagion

$X_{-i} \rightarrow$ Investments of other organisations in the community

8.2 Acronyms used in the thesis:

DP $\rightarrow$ Dynamic Programming

GA $\rightarrow$ Genetic Algorithm

RA $\rightarrow$ Risk assessment

CARA $\rightarrow$ Constant Absolute Risk Aversion

CRRA $\rightarrow$ Constant Relevant Risk Aversion

CVSS $\rightarrow$ Common Vulnerability Scoring System

Bibliography

[1] Cyber Insurance: Risks and trends 2020, MunichRE, 2020.

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

[3] Symantec: Internet Security Report. Volume 24. Available on `https://docs.broadcom.com/doc/istr-24-2019-en`, 2019

[4] Phil McCausland, Sam Petulla and Alastair Jamieson. Global Cyberattack Hits 150 Countries. Available on https://www.nbcnews.com/tech/internet/after-huge-global-cyberattack-countries-scramble-halt-spread-ransomware-n759121, 2017

[5] Ivan Homoliak, Flavio Toffalini, Juan Guarnizo, Yuval Elovici, and Martín Ochoa. "Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures." ACM Computing Surveys (CSUR) 52, no. 2: pp. 1–40, 2019.

[6] Cisco: Annual Cybersecurity Report. Available on `http://www.cisco.com/go/acr2017`, 2017.

[7] Ponemon Institute and IBM: Cost of a Data Breach Report. Available on https://www.ibm.com/security/digital-assets/cost-data-breach-report/, 2020.

[8] Richard A.Caralli, James F.Stevens, Lisa R.Young, and William R.Wilson. Introducing octave allegro: Improving the information security risk assessment process. No. CMU/SEI-2007-TR-012. Carnegie–Mellon Univ Pittsburgh PA Software Engineering Inst, 2007.

[9] NIST, Security and Privacy Controls for Federal Information Systems and Organizations, Tech. Rep. SP 800–53 Revision 4, National Institute of Standards and Technology, 2013.

[10] HIPAA: The Health Insurance Portability and Accountability Act. Available on `https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html`, 1996

[11] GDPR: General Data Protection Regulation. Available on `https://gdpr-info.eu/`, 2016.

[12] Miguel A.Amutio, Javier Candau, and José Manás. "Magerit-version 3, methodology for information systems risk analysis and management, book I-the method." Ministerio de administraciones públicas, 2014.

[13] Mass Soldal Lund, Bjørnar Solhaug, and Ketil Stølen. Model-driven risk analysis: the CORAS approach. Springer Science & Business Media, 2010.

[14] Bilge Karabacak and Ibrahim Sogukpinar. ISRAM: Information Security Risk Analysis Method. Computers 4 Security, 24(2):147–159, 2005.

[15] Quey-Jen Yeh and Arthur Jung-Ting Chang. Threats and countermeasures for information system security: A cross-industry study. Inf. Manage., 44(5):480–491, 2007.

[16] A. Jürgenson and J. Willemson. Serial model for attack tree computations. In Information, Security and Cryptology–ICISC2009, pages 118–128. Springer, 2010.

[17] Miles A.McQueen, 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.

[18] NIST (National Institute of Standards and Technology). National Vulnerability Database (NVD). Available on `https://nvd.nist.gov/`

[19] William Nzoukou, 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.

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

[21] PwC: Global Cyber Insurance Survey. Available on `https://www.pwc.com/us/en/industries/insurance/library/cyber-insurance-survey.html`, 2018.

[22] Lawrence A.Gordon and Martin P.Loeb. Managing cybersecurity resources: a cost-benefit analysis. Vol. 1. New York: McGraw-Hill, 2006.

[23] Gary Stoneburner, Alice Goguen, and Alexis Feringa. Risk management guide for information technology systems. Technical Report 800-30, National Institute of Standards and Technology, 2001. Available on http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf on 2009.

[24] Lawrence A.Gordon, and Martin P. Loeb. "Return on information security investments: Myths vs. realities." Strategic finance 84, no. 5, 2002.

[25] Angelica Marotta, Fabio Martinelli, Stefano Nanni, Albina Orlando and Artsiom Yautsiukhin. Cyber–insurance survey. Computer Science Review 24, pp. 35–61, 2017

[26] PartnerRe: Survey of Cyber Insurance Market Trends, Available on `https://partnerre.com/`, 2019.

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

[28] 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.

[29] Mohammad Mahdi Khalili, 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.

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

[31] Parinaz Naghizadeh, and Mingyan Liu. "Voluntary participation in cyber-insurance markets." In Workshop on the Economics of Information Security (WEIS). 2014.

[32] Fabio Massacci, Joseph Swierzbinski and Julian Williams. "Cyberinsurance and Public Policy: Self-Protection and Insurance with Endogenous Security Risks." In 16th Annual Workshop on the Economics of Information Security: WEIS, 2017.

[33] Savino Dambra, Leyla Bilge and Davide Balzarotti. "SoK: Cyber Insurance—Technical Challenges and a System Security Roadmap." In 2020 IEEE Symposium on Security and Privacy (SP), pp. 293–309, 2020.

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

[35] Hulisi Ogut, Nirup Menon and Srinivasan Raghunathan: Cyber insurance and it security investment: Impact of interdependent risk. In: Proceedings of the 4^{th} Workshop on the Economics of Information Security, 2005.

[36] Bruce Schneier. "Insurance and the computer industry." Communications of the ACM 44, no. 3, 2001.

[37] Rainer Böhme, Stefan Laube and Markus Riek. "A fundamental approach to cyber risk analysis." Variance 12, no. 2: pp. 161–185, 2019.

[38] Ranjan Pal, Leana Golubchik, Konstantinos Psounis and Pan Hui. "Will cyber-insurance improve network security? A market analysis." In IEEE INFOCOM 2014-IEEE Conference on Computer Communications, pp. 235-243. IEEE, 2014.

[39] Ross Anderson, Rainer Böhme, Richard Clayton and Tyler Moor. "Security economics and European policy." In ISSE 2008 Securing Electronic Business Processes, pp. 57-76. Vieweg+ Teubner, 2009.

[40] Ruperto P.Majuca, William Yurcik and Jay P.Kesan.: The evolution of cyberinsurance. The Computing Research Repository pp. 1–16, 2006.

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

[42] Stefanos Gritzalis, Athanasios N.Yannacopoulos, Costas Lambrinoudakis, Petros Hatzopoulos and Sokratis K.Katsikas. "A probabilistic model for optimal insurance contracts against security risks and privacy violation in IT outsourcing environments." International Journal of Information Security 6, no. 4, pp. 197–211, 2007.

[43] Nikhil Shetty, Galina Schwartz, Mark Felegyhazi and Jean Walrand. "Competitive cyber-insurance and internet security." In Economics of information security and privacy, pp. 229-247. Springer, Boston, MA, 2010.

[44] Galina Schwartz, and Shankar Sastry. "Cyber-insurance framework for large scale interdependent networks." In Proceedings of the 3rd international conference on High confidence networked systems, pp. 145-154. 2014.

[45] Arunabha Mukhopadhyay, Samir Chatterjee, Kallol K. Bagchi, Peteer J. Kirs, and Girja K. Shukla. "Cyber risk assessment and mitigation (CRAM) framework using logit and probit models for cyber insurance." Information Systems Frontiers 21, no. 5 (2019): 997-1018.

[46] Sasha Romanosky, Lillian Ablon, Andreas Kuehn, and Therese Jones. "Content analysis of cyber insurance policies: how do carriers price cyber risk?." Journal of Cybersecurity 5, no. 1, 2019.

[47] Shauhin A.Talesh. "Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses." Law & Social Inquiry 43, no. 2, pp. 417-440, 2018.

[48] Zichao Yang and John CS Lui. "Security adoption and influence of cyber-insurance markets in heterogeneous networks." Performance Evaluation 74, pp. 1-17, 2014.

[49] Marc Lelarge and Jean Bolot. "Network externalities and the deployment of security features and protocols in the internet." ACM SIGMETRICS Performance Evaluation Review 36, no. 1, pp. 37-48, 2008.

[50] Xia Zhao, Ling Xue and Andrew B.Whinston. "Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements." Journal of Management Information Systems 30, no. 1, pp. 123-152, 2013.

[51] Travel insurance through Europ Assistance. Available on https://www.europ-assistance.com/.

[52] Chun-Jen Chung, Pankaj Khatkar, Tianyi Xing, Jeongkeun Lee and Dijiang Huang. "NICE: Network intrusion detection and countermeasure selection in virtual network systems." IEEE transactions on dependable and secure computing 10, no. 4 : pp. 198-211, 2013.

[53] John J.Bartholdi III. "The knapsack problem." In Building intuition, pp. 19–31. Springer, Boston, MA, 2008.

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

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

[56] Rinku Dewri, Indrajit Ray, Nayot Poolsappasit and Darrell Whitley. "Optimal security hardening on attack tree models of networks: a cost-benefit analysis." International Journal of Information Security 11, no. 3: pp. 167-188, 2012.

[57] Yunghee Lee, Tae Jong Choi and Chang Wook Ahn. "Multi-objective evolutionary approach to select security solutions." CAAI Transactions on Intelligence Technology 2, no. 2: pp. 64-67, 2017.

[58] Iryna Yevseyeva, Vitor Basto-Fernandes, Michael Emmerich and Aad van Moorsel. "Selecting optimal subset of security controls." Procedia Computer Science 64, pp. 1035-1042, 2015.

[59] Iryna Yevseyeva, Vitor Basto Fernandes, Aad van Moorsel, Helge Janicke and Michael Emmerich. "Two-stage security controls selection." Procedia Computer Science 100, pp. 971-978, 2016.

[60] Valentina Viduto, Carsten Maple, Wei Huang and David LoPez-PereZ. "A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem." Decision Support Systems 53, no. 3: pp. 599-610, 2012.

[61] Valentina Viduto, Carsten Maple, Wei Huang and Alexey Bochenkov. "A multi-objective genetic algorithm for minimising network security risk and cost." In 2012 International Conference on High Performance Computing & Simulation (HPCS), pp. 462-467. IEEE, 2012.

[62] Kumar, Rajeev, and Nilanjan Banerjee. "Analysis of a multiobjective evolutionary algorithm on the 0–1 knapsack problem." Theoretical Computer Science 358, no. 1, pp. 104-120, 2006.

[63] Lust, Thibaut, and Jacques Teghem. "The multiobjective multidimensional knapsack problem: a survey and a new approach." International Transactions in Operational Research 19, no. 4, pp. 495-520, 2012.

[64] Jeffrey Horn, Nicholas Nafpliotis, and David E. Goldberg. "A niched Pareto genetic algorithm for multiobjective optimization." In Proceedings of the first IEEE conference on evolutionary computation, IEEE world congress on computational intelligence, vol. 1, pp. 82-87. 1994.

[65] Andrew Fielder, Emmanouil Panaousis, Pasquale Malacaria, Chris Hankin and Fabrizio Smeraldi. "Decision support approaches for cyber security investment." Decision support systems 86: pp. 13–23, 2016.

[66] Silvano Martello, David Pisinger and Paolo Toth. "Dynamic programming and strong bounds for the 0-1 knapsack problem." Management Science 45, no. 3, pp. 414–424, 1999.

[67] Paolo Toth. "Dynamic programming algorithms for the zero-one knapsack problem." Computing 25, no. 1, pp. 29–45, 1980.

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

[69] Sami Khuri, Thomas Bäck and Jörg Heitkötter. "The zero/one multiple knapsack problem and genetic algorithms." In Proceedings of the 1994 ACM symposium on Applied computing, pp. 188-193, 1994.

[70] Darrell Whitley. "A genetic algorithm tutorial." Statistics and computing 4, no. 2, pp. 65–85, 1994.

[71] Ahmad Hassanat, V.Prasath, Mohammed Abbadi, Salam Abu-Qdari, and Hossam Faris. "An improved genetic algorithm with a new initialization mechanism based on regression techniques." Information 9, no. 7, 2018.

[72] Nikolaj Goranin and Antanas Cenys. "Genetic algorithm based Internet worm propagation strategy modeling under pressure of countermeasures." Journal of Engineering Science & Technology Review 2, no. 1, 2009.

[73] Suhail Owais, Vaclav Snasel, Pavel Kromer and Ajith Abraham. "Survey: using genetic algorithm approach in intrusion detection systems techniques." In 2008 7^{th} Computer Information Systems and Industrial Management Applications, pp. 300-307. IEEE, 2008.

[74] 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, pp. 211-229, 1993.

[75] ISO/IEC 27002:2013 — Information technology — Security techniques — Code of practice for information security controls (second edition), 2013.

[76] Alex J.Smola and Bernhard Scholkopf. Sparse greedy matrix approximation for machine learning. In Proceedings of the International Conference on Machine Learning, pp. 911–918, San Francisco, Morgan Kaufmann Publishers, 2000.

[77] Nerijus Paulauskas and Eimantas 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.

[78] E. Rescorla, "Is Finding Security Holes a Good Idea?" IEEE Security & Privacy, vol. 3, no. 1, pp. 14–19, 2005.

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

[80] ENISA: Incentives and barriers of the cyber insurance market in europe. Available on `http://www.goo.gl/BtNyj4on12/12/2014`, 2012.

[81] National Protection and Programs Directorate. Department of Homeland Security, Cybersecurity insurance workshop readout report, Available on https://www.dhs.gov/sites/default/files/publications/cybersecurity-insurance-read-out-report.pdf, 2012.

[82] Murray Turoff and Harold A. Linstone. "The Delphi method-techniques and applications.", 2002.

[83] Chia-Chien Hsu and Brian A.Sandford. "The Delphi technique: making sense of consensus." Practical Assessment, Research, and Evaluation 12, no. 1, 2007.

[84] CLUSIF. Mehari 2010. Risk analysis and treatment guide. Club De La Securite De L'Information Francias, 2010.

[85] CLUSIF. Mehari 2010. Processing guide for risk analysis and management. Club De La Securite De L'Information Francias, 2 edition, 2011.

[86] Fariborz Farahmand, Shamkant B.Navathe, Philip H.Enslow and Gunter P.Sharp. "Managing vulnerabilities of information systems to security incidents." In Proceedings of the 5th international conference on Electronic commerce, pp. 348-354. 2003.

[87] Hennie A.Kruger and Wayne D.Kearney. "A prototype for assessing information security awareness." Computers & security 25, no. 4, pp. 289-296, 2006.

[88] Quey-Jen Yeh and Arthur Jung-Ting Chang. "Threats and countermeasures for information system security: A cross-industry study." Information & Management 44, no. 5, pp. 480-491, 2007.

[89] Dai Nishioka, Yuko Murayama and Yasuhiro Fujihara. "Producing a questionnaire for a user survey on anshin with information security for users without technical knowledge." In 2012 45th Hawaii International Conference on System Sciences, pp. 454-463. IEEE, 2012.

[90] ADVISEN: Loss Data Insight. Available on `https://www.advisenltd.com/data/loss-data/`, 2019.

[91] AIG Asia Pacific Insurance Pte. Ltd. Cyberedge supplementary questionnaire - cyber insurance, 2013. Available on `http://www.aig.com.sg/chartisint/internet/SG/en/files`.

[92] Rainer Böhme and Galina Schwartz. "Modeling Cyber-Insurance: Towards a Unifying Framework." In WEIS, 2010.

[93] Benjamin Johnson, Aron Laszka and Jens Grossklags. "How many down?: toward understanding systematic risk in networks." In Proceedings of the 9th ACM symposium on Information, computer and communications security, pp. 495-500. ACM, 2014.

[94] Michael Rothschild and Joseph E.Stiglitz. Equilibrium in competitive insurance markets: An essay on the economics of imperfect information. The Quarterly Journal of Economics, 90(4): pp. 630–49, 1976.

[95] George A.Akerlof. "The market for "lemons": Quality uncertainty and the market mechanism." In Uncertainty in economics, pp. 235-251. Academic Press, 1978.

[96] Ramaswamy Chandramouli. Security Strategies for Microservices-based Application Systems. No. Special Publication (NIST SP)-800-204, 2019.

[97] Ramaswamy Chandramouli, Murugiah Souppaya, and Karen Scarfone. NIST Guidance on Application Container Security. No. ITL Bulletin October 2017. National Institute of Standards and Technology, 2017.

[98] ISO/IEC, ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management (third edition), 2018.

[99] R.S. Betterley, Cyber/privacy insurance market survey, Available on http://betterley.com/samples/cpims14_nt.pdf, 2014.

[100] Costis Toregas, and Nicolas Zahn. "Insurance for cyber attacks: The issue of setting premiums in context." George Washington University, 2014.

[101] Maya Hristakeva, and Dipti Shrestha. "Solving the 0-1 knapsack problem with genetic algorithms." In Midwest instruction and computing symposium, 2004.

[102] Anton Iliev, Nikolay Kyurkchiev, Asen Rahnev, and Todorka Terzieva. "Some models in the theory of computer viruses propagation." LAP LAMBERT Academic Publishing, 2019.

[103] Loren Paul Rees, Jason K. Deane, Terry R. Rakes, and Wade H. Baker. "Decision support for Cybersecurity risk planning." Decision Support Systems 51, no. 3: pp. 493–505, 2011.

[104] Megha Gupta. "A fast and efficient genetic algorithm to solve 0–1 knapsack problem." Int J Digit Appl Contemp Res 1, no. 6: pp. 1-5, 2013.

[105] Herbert A Simon. The sciences of the artificial. MIT press, 2019.

[106] Humza Naseer, Graeme Shanks, Atif Ahmad, and Sean Maynard. "Towards an analytics-driven information security risk management: A contingent resource based perspective.", 2017.

[107] Arunabha Mukhopadhyay, Samir Chatterjee, Debashis Saha, Ambuj Mahanti, and Samir K. Sadhukhan. "Cyber-risk decision models: To insure IT or not?." Decision Support Systems 56: pp. 11-26, 2013.

[108] Mohammad Mahdi Khalili, Mingyan Liu, and Sasha Romanosky. "Embracing and controlling risk dependency in cyber-insurance policy underwriting." Journal of Cybersecurity 5, no. 1, 2019.

[109] Ross Anderson, and Tyler Moore. "The economics of information security." Science 314, no. 5799, pp. 610-613, 2006.

[110] Christian Biener, Martin Eling, and Jan Hendrik Wirfs. "Insurability of cyber risk: An empirical analysis." The Geneva Papers on Risk and Insurance-Issues and Practice 40, no. 1, pp. 131-158, 2015.

[111] ISO/IEC, ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements, 2013.

[112] Cybersecurity, Critical Infrastructure. "Framework for Improving Critical Infrastructure Cybersecurity." Framework 1, 2014.

[113] Ranjan Pal, and Pan Hui. "Cyberinsurance for cybersecurity a topological take on modulating insurance premiums." ACM SIGMETRICS Performance Evaluation Review 40, no. 3, pp. 86-88, 2012.

[114] Böhme, Rainer, and Gaurav Kataria. "Models and Measures for Correlation in Cyber-Insurance." In WEIS. 2006.

[115] Lawrence A.Gordon, Martin P. Loeb, and Tashfeen Sohail. "A framework for using insurance for cyber-risk management." Communications of the ACM 46, no. 3, pp. 81-85, 2003.

[116] Woohyun Shim. "An analysis of information security management strategies in the presence of interdependent security risk." Asia Pacific Journal of Information Systems 22, no. 1, pp. 79-101, 2012.

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

[118] Moore, Tyler. "The economics of cybersecurity: Principles and policy options." International Journal of Critical Infrastructure Protection 3, no. 3-4, pp. 103-117, 2010.

[119] Herath HS, Herath TC. Cyber-Insurance: Copula Pricing Framework and Implication for Risk Management. In WEIS, 2007.

[120] David Pisinger. "Algorithms for knapsack problems.", 1995.

[121] S. Bistarelli, M. Dall'Aglio, and P. Peretti. Strategic games on defense trees. In Proceedings of 4th International Workshop on Formal Aspects in Security and Trust, pages 1–15, 2007.

[122] Stefano Bistarelli, Pamela Peretti, and Irina Trubitsyna. "Analyzing security scenarios using defence trees and answer set programming."

Electronic Notes in Theoretical Computer Science 197, no. 2, pp. 121-129, 2008.

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

[124] Fabio Martinelli, and Artsiom Yautsiukhin. "Security by insurance for services." In 2016 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), pp. 344-351. IEEE, 2016.

[125] Maria Francesca Carfora, Fabio Martinelli, Francesco Mercaldo, Albina Orlando, and Artsiom Yautsiukhin. "Cyber Risk Management: A New Challenge for Actuarial Mathematics." In Mathematical and Statistical Methods for Actuarial Sciences and Finance, pp. 199-202. Springer, Cham, 2018.