A Decision Making Method for Selection of Security Controls based on Cost-Effectiveness Analysis and Modeling

MSc Thesis by Tuan Khoa Pham
August 2017
Acknowledgements

Above all, I wish to thank my main supervisor Aida Omerovic, scientist and researcher at SINTEF ICT, for her tremendous support and dedication. Aida has always remained enthusiastic and patient, guided me through the thesis work with her immense knowledge.

I would like to express my sincere gratitude to my co-supervisors Professor Ketil Stølen, Chief scientist at SINTEF ICT, together with my former co-supervisors Knut Håkon Merch, Director at Deloitte Norway, for their expertise, motivation and valuable feedback.

I am also grateful to Marit Ruud McGhie, my first and best Norwegian teacher at the University of Oslo, who gave me the key for understanding Norwegian language and culture, as well as my colleagues and fellow students for their participation, insightful comments and discussions during the research of this thesis.

Finally, to my family with love and gratefulness, for their incredible support and encouragement throughout my study and daily life.

Oslo, 1 August 2017

Tuan Khoa Pham
Abstract

Nowadays, the issues around Information Security no longer stand on their own but are shifting from what is technically possible to what is economically efficient [19]. Indeed, Anderson [2] has claimed that many of the problems can be explained more clearly and convincingly using the language of microeconomics. Moreover, it has always been demanding to balance between the cost and the benefit gained from the selection of security controls corresponding to risks and vulnerabilities.

As we have discussed in the problem analysis of this thesis, there are still many challenges regarding decision making process in the context of Information Security that include (1) risk assessment, (2) security controls analysis, and (3) selection of security controls to mitigate risks in a cost-effective manner. For that reason, the goal of our proposed thesis is to develop a decision making method that supports the selection of security controls, in the way that it would be easier for security consultants and organization to make sufficient security investment and strengthen their security baseline.

In order to achieve the overall research objective, this thesis contributes with four main artifacts grounded on its set of success criteria: (1) The checklist for security consultants, (2) The tool support, (3) The process of decision making method, and (4) The approach to cost-effectiveness modeling. These success criteria help us to design and evaluate the results as well as the success of our research at later state. Besides, case study and technology research that provide sufficient degree of generality, precision and realism have been chosen as research method for conducting the research. The results gained from the evaluation through case study include a list of suggested security controls with corresponding estimated costs, expected effect and benefit, together with cost-effectiveness models showing correlation between the risk picture and total cost of implementation.

This MSc thesis contributes to the domain of risk assessment and selection of security controls. In the end, we hope that our findings and result can be utilized in the development of decision making method for selection of security controls in the context of cybersecurity investment.

**Keywords**: checklist for security consultants, risk assessment, cost-effectiveness models, decision making method, security risk controls, cybersecurity investment.
List of figures

Figure 3.1.: Method for technology research (adopted from Solheim and Stølen [15]) ..........11
Figure 3.2.1: Strategies for evaluation (adopted from McGrath [27]) ........................................13
Figure 3.6: Research method (adopted from Refsdal [46] and modified) .................................16
Figure 3.6.1: Responses received sorted by date ..................................................................17
Figure 4.2.5: Cyber Kill Chain (adopted from Lockheed Martin [47]) ..................................25
Figure 4.4: Risk aversion illustrated by Utility function (adopted from Policonomics [37]) ...29
Figure 5: The relationship between artifacts ........................................................................33
Figure 5.2.1a: The tool support components .........................................................................37
Figure 5.2.1b: General Information ......................................................................................37
Figure 5.2.1c: Asset Register ..................................................................................................39
Figure 5.2.1d: Threat Agent Register ....................................................................................39
Figure 5.2.1e: Vulnerability Register .....................................................................................39
Figure 5.2.1f: Risk Register ....................................................................................................40
Figure 5.2.1g: Remediation Plan .........................................................................................40
Figure 5.3: The process of decision making method overview ..............................................42
Figure 5.4.1: Cost-effectiveness model based on CKS .........................................................45
Figure 5.4.2: Cost-effectiveness model based on CSF (Demo data) ....................................47
Figure 5.4.3: Cost-effectiveness model based on CSC (Demo data) ....................................48
Figure 6.4.1: Cyber Kill Chain and suggested controls .........................................................69
Figure B.G.1: Are you IT security consultant? .....................................................................97
Figure B.G.2: Location (for IT Consultants) .........................................................................97
Figure B.G.3.1: Education (for IT Consultants) .....................................................................98
Figure B.G.3.2: Professional experiences (for IT Consultants) ..........................................99
Figure B.G.4: Location (for Organization) .............................................................................99
Figure B.M.1: Question 1 results ..........................................................................................101
Figure B.M.2: Question 2 results ..........................................................................................102
Figure B.M.3: Question 3 results ..........................................................................................103
Figure B.M.4: Question 4 results ..........................................................................................103
Figure B.M.5: Question 5 results ..........................................................................................104
Figure B.M.6: Question 6 results ..........................................................................................105
Figure B.M.7: Question 7 results ..........................................................................................105
Figure B.M.8: Question 8 results ..........................................................................................106
Figure B.M.9: Question 9 results ..........................................................................................107
Figure B.M.10: Question 10 results ....................................................................................107
Figure B.M.11: Question 11 results .....................................................................................108
Figure B.M.12: Question 12 results .....................................................................................109
List of tables

Table 4.2.1: Attackers’ attributes (adapted from INTEL TAL [17]) .......................................................... 22
Table 2.1: Cybersecurity Framework Core Outcome (adopted from NIST [4]) ........................................ 26
Table 5.3.1: The overview of the process ................................................................................................. 44
Table 5.4.2: Cost-effectiveness data based on CSF (Demo data) .............................................................. 47
Table 5.4.3: Cost-effectiveness data based on CSC (Demo data) ............................................................. 48
Table 6.1.2: Intrusion Attempts Indicators (adopted from Hutchins [48]) ................................................... 54
Table 6.3.1.1: General Information (Result from Tool support) .............................................................. 55
Table 6.3.1.2a: The first areas from ISO 27001:2013 (Result from Tool support) ......................... 56
Table 6.3.1.2b: The first 13 Incident Scenarios from SANS (Result from Tool support) ................. 57
Table 6.3.1.2c: Lockheed Martin Cyber Kill Chain (Result from Tool support) ........................... 57
Table 6.3.1.2d: NIST Cybersecurity Framework (Result from Tool support) .................................... 58
Table 6.3.1.2e: Control Area 8 from CIS CSC Top 20 (Result from Tool support) ........................... 58
Table 6.3.1.3a: Asset Register (Result from Tool support) ................................................................. 59
Table 6.3.1.3b: Classification of Personal Information ........................................................................ 59
Table 6.3.1.3c: Consequence scale for A1 .............................................................................................. 60
Table 6.3.1.3d: Consequence scale for A2 .............................................................................................. 60
Table 6.3.1.3e: Consequence scale for A3 .............................................................................................. 60
Table 6.3.1.3f: Consequence scale for A4 .............................................................................................. 60
Table 6.3.1.3g: Threat Agent Register (Result from Tool support) ...................................................... 61
Table 6.3.1.3h: Vulnerability Register (Result from Tool support) ....................................................... 62
Table 6.3.1.3i: Classification of Likelihood ............................................................................................ 62
Table 6.3.1.3j: Classification of severity ............................................................................................... 62
Table 6.3.1.3k: Acceptance criteria for risks ......................................................................................... 63
Table 6.3.1.3l: Description of Risk acceptance criteria ........................................................................ 63
Table 6.3.1.3m: Risk Register .............................................................................................................. 63
Table 6.3.1.3n: Remediation Plan ........................................................................................................ 64
Table 6.4a: Register vulnerabilities (Assumed data) .............................................................................. 66
Table 6.4b: Suggested controls mapping towards vulnerabilities (Assumed data) ............................. 66
Table 6.4c: Register vulnerabilities mapping towards CSC, CSF and CKC ................................... 67
Table 6.4d: Suggested controls mapping towards CSC, CSF and CKC ............................................. 68
Table 6.4.2: Vulnerabilities per CSF and related costs ..................................................................... 69
Table 6.4.3: Vulnerabilities per CSC and related costs .................................................................... 70
Contents

Acknowledgements i
Abstract iii
List of figures v
List of tables vi

Chapter 1
Introduction 1

1.1. Research focus ................................................................. 1
   1.1.1. Problem ......................................................................... 1
   1.1.2. Objective .................................................................. 2

1.2. Contribution ........................................................................ 2
   1.2.1. The checklist for security consultants ................................. 2
   1.2.2. The tool support for the decision making method .................. 3
   1.2.3. The process of decision making method ............................... 3
   1.2.4. The approach to cost-effectiveness modeling ........................ 4

1.3. Thesis structure .................................................................. 4

Chapter 2
Identifying needs 7

2.1. Stakeholders ....................................................................... 7
   2.1.1. Security consultants....................................................... 7
   2.1.2. Decision makers .......................................................... 8

2.2. Success criteria .................................................................... 8
   2.2.1. The checklist for security consultants ................................. 9
   2.2.2. The tool support for the decision making method .................. 9
   2.2.3. The process of decision making method ............................... 10
   2.2.4. The approach to cost-effectiveness modeling ........................ 10

Chapter 3
Research method 11

3.1. Research method ................................................................. 11

3.2. Strategies for evaluation ...................................................... 12
   3.2.1. Overview of strategies ................................................. 12
### 3.2.2. Case study ........................................................................................................13

### 3.3. Selection of evaluation method ...........................................................................13

### 3.4. Empirical data collection .....................................................................................14

#### 3.4.1. Interview ...........................................................................................................14

#### 3.4.2. Observation ......................................................................................................14

#### 3.4.3. Questionnaire ....................................................................................................14

#### 3.4.4. Literature research ............................................................................................15

### 3.5. Selection of empirical data collection method.....................................................15

### 3.6. How we have applied selected research method ................................................15

#### 3.6.1. The checklist for security consultants & The tool support ............................17

#### 3.6.2. The process of the decision making method ...................................................18

#### 3.6.3. The approach to cost-effectiveness models .....................................................18

---

**Chapter 4
State of the art**

19

#### 4.1. Risk assessment standards ...............................................................................19

##### 4.1.1. ISO 27000 family .........................................................................................19

##### 4.1.2. ISO 31000 family .........................................................................................19

##### 4.1.3. NIST SP 800-30 ..........................................................................................20

#### 4.2. Risk analysis approaches .................................................................................20

##### 4.2.1. INTEL Threat Agent Library (TAL) ............................................................20

##### 4.2.2. CORAS and PREDIQT ..............................................................................22

##### 4.2.3. Lockheed Martin Cyber Kill Chain (CKC) ....................................................23

##### 4.2.4. NIST Cybersecurity Framework (CSF) .........................................................25

##### 4.2.5. CIS Critical Security Controls (CSC) ........................................................26

#### 4.3. Microeconomics models ....................................................................................27

#### 4.4. Decision theory ..................................................................................................28

#### 4.5. Tool support & Development environments ....................................................30

##### 4.5.1. Excel spreadsheets .........................................................................................30

##### 4.5.2. RSA Archer ..................................................................................................30

##### 4.5.3. CORAS tool ..................................................................................................31

##### 4.5.4. GNU Octave ................................................................................................31

---

**Chapter 5
Artifacts**

33
5.1. The checklist for security consultants ................................................................. 34
  5.1.1. Identifying ........................................................................................................ 34
  5.1.2. Estimating ........................................................................................................ 35
  5.1.3. Selecting .......................................................................................................... 36
5.2. The tool support for the decision making method .................................................. 36
  5.2.1. The design and components of the tool support .............................................. 37
  5.2.2. How to use the tool ......................................................................................... 41
5.3. The process of decision making method ............................................................... 41
  5.3.1. The overview of the process .......................................................................... 43
  5.3.2. How the checklist and tool support are used in this process ......................... 43
5.4. The approach to cost-effectiveness modeling ...................................................... 44
  5.4.1. Cost-effectiveness model based on Cyber Kill Chain ...................................... 45
  5.4.2. Cost-effectiveness model based on Cybersecurity Framework ...................... 46
  5.4.3. Cost-effectiveness model based on Critical Security Controls Top 20 .......... 47

Chapter 6
Evaluation of artifacts 51

6.1. Case description .................................................................................................. 51
  6.1.1. The organization .............................................................................................. 51
  6.1.2. The case background ....................................................................................... 51
  6.1.3. The context ...................................................................................................... 52
  6.1.4. The risk picture ............................................................................................... 52
6.2. The checklist and tool support for the decision making method ......................... 54
6.3. The process of decision making method ............................................................... 55
  6.3.1. Applying the checklist with tool support ............................................................ 55
6.4. The approach to cost-effectiveness modeling ...................................................... 65
  6.4.1. Cost-effectiveness model based on Cyber Kill Chain ...................................... 68
  6.4.2. Cost-effectiveness model based on Cybersecurity Framework ...................... 69
  6.4.3. Cost-effectiveness model based on Critical Security Controls Top 20 .......... 69
6.5. The output of the process of decision method ...................................................... 71
6.6. Observations during case study ........................................................................... 72

Chapter 7
Evaluation with respect to success criteria 73

7.1. The checklist for security consultants ................................................................. 73
7.2. The tool support for decision making method ................................................................. 74
7.3. The process of decision making method ........................................................................... 75
7.4. The approach to cost-effectiveness modeling ................................................................. 75

Chapter 8
Threats to validity and reliability 77

8.1. Threats to validity ........................................................................................................... 77
   8.1.1. Construct validity ...................................................................................................... 77
   8.1.2. Internal validity ........................................................................................................ 78
   8.1.3. External validity ...................................................................................................... 78

8.2. Threats to reliability ...................................................................................................... 78

Chapter 9
Conclusions and Future work 81

9.1. Lesson learned .............................................................................................................. 81
9.2. Conclusions .................................................................................................................. 82
9.3. Future work .................................................................................................................. 83

Bibliography 87

Appendices 91

A. Questionnaire ................................................................................................................ 91
   Introduction ...................................................................................................................... 91
   Objective ......................................................................................................................... 91
   General questions .......................................................................................................... 91
   Multiple Choice Questions ........................................................................................... 92

B. Results from Questionnaire ........................................................................................... 97
   General questions .......................................................................................................... 97
   Multiple Choice Questions ......................................................................................... 101

C. Terminology .................................................................................................................. 113
Chapter 1

Introduction

According to Anderson [1], Information Security is traditionally implemented as an afterthought, and security solutions as a result are often reactive rather than proactive. Indeed, accomplishing the goals in order to achieve highest economic results is supposed to be one of the most important factors in many business sectors. It is the focus on productivity, or in other words, to get the job done right within the budget rather than to get it done in a secure manner.

Lately, the interest of economic growth from the Information Security aspects has been increasing remarkably. People begin to realize that the damage caused by lack of efficient controls is far greater than the cost of implementing them [1]. From the business perspective, cost-benefit analysis within Information Security begins to gain more focus. However, it has always been a challenge to balance between the cost to analyze and invest in a security system and the benefit gained from that process.

Information Security, in relation to normal security, is hard to implement [2]. From the economic perspective, Anderson [2] has also claimed that many of the problems can be explained more clearly and convincingly using the language of microeconomics. In that manner, Information Security investment has become an interesting but challenging concern for every business and enterprise. What kind of security controls are missing and should be invested? How much is enough? What is the cost and the corresponding benefit gained from the investment? Is there any model that could help business while making such decision?

1.1. Research focus

1.1.1. Problem

The issues around Information Security no longer stand on their own but are shifting from what is technically possible to what is economically efficient [19]. As per now, we can figure out that there is still a limitation in the market on what security consultants and organizations can cooperate to achieve cost-effect in the field of Information Security investment. There is a lack of
sufficient decision making method that combines risk analysis, security controls and cost-effectiveness, together with a tool support that works as a guideline for security consultants as well as organizations. On the one hand, security consultants are still missing information about industry standards and guidelines regarding risk analysis. On the other hand, organizations often have to seek for advice how much benefit they can gain from security controls, whether security investment is worth the money, and how their security situation will be improved.

1.1.2. Objective

The main objective of this thesis is to develop a decision making method that supports the selection of security controls and cost-effectiveness analysis in the context of security risk assessment. The method should be:

- useful in the sense that the suggestions of security controls based on its cost and benefit are sufficient;
- comprehensible for the involved stakeholders; and
- cost-effective

In that way it would be easier for security consultants and organizations to make sufficient and cost-effective security investment. The expected result should be the increase in the value of reliability regarding risk assessment and selection of security controls, as well as the security maturity of organizations.

1.2. Contribution

The contribution of this thesis is to facilitate the decision making method regarding risk assessment and the selection of security controls based on a cost-effectiveness analysis. In order to achieve the main objective mentioned above, in this thesis we focus on the following artifacts:

1.2.1. The checklist for security consultants

There are many methods out there in the market that have been using to implement risk assessment. The point here is to understand what should be and has been using lately in the industry. A questionnaire is created for this purpose. Collected information is processed anonymously for the sake of privacy. The checklist itself is composed of three main groups: (1) Identifying, (2) Estimating, and (3) Selecting where each group contains a set of bullet points. The name of each group expresses the function of all bullet points in the group. The purpose of
the checklist is to guide security consultants throughout each phase of the decision making method. The checklist is developed based on the questionnaire and evaluated by collecting answers from a selected group of security domain experts.

Detailed information about the questionnaire, collected responses and written feedbacks are presented in Appendix A and Appendix B.

1.2.2. The tool support for the decision making method

The tool support, developed based on the checklist, is aimed to be used by security consultants and organizations to register: (1) assets, (2) threat agents, (3) vulnerabilities, (4) risks, (5) suggested controls, expected effect and benefit while conducting the risk assessment. The tool also contains a «Metadata» section where information from some of the most lately used standards and guidelines has been collected. Security consultants use the «Metadata» as reference during the decision making process.

The tool support should fulfill the following requirements: (1) user friendly, easy to use and maintain, (2) could be use as a template, (3) could store metadata, i.e. industry standards, guidelines etc., (4) could show which security controls are in place, (5) could provide differences in the price while choosing different security controls based on its effect.

1.2.3. The process of decision making method

A process is meant to be an order of activities that are conducted to acquire a certain objective. The process needs clearly identified input in order to create sufficient output.

The security consultants are the ones that manage the risk assessment and cost-effectiveness analysis. They lead the process, understand the needs of organizations, and document the results. The whole process should be sufficient and the results should be correct and reliable. A list of security controls used as treatments to reduce risks are expected as the output of this process. The security consultants will then implement the cost-effectiveness modeling.

This process of decision making method has been developed tightly together with the checklist and tool support. The result is a six-phases-process as illustrated in figure 5.3 in chapter 5. The process facilitates and systematically guides security consultants throughout the conduct of risk assessment, estimating cost - effect - benefit of suggested controls, visualizing the results in order to provide organizations a clearer risk picture and its correlation with the total cost of controls implementation.
It is important that security consultants work closely with the organizations, help them to understand the risks, the corresponding security controls and the expected effect so that organizations are able to make sufficient decision on how they should invest in security.

1.2.4. The approach to cost-effectiveness modeling

A modeling approach is meant to provide a complete set of models with a pre-defined purpose. A modeling approach should contain clear syntax, i.e., notation; semantics, i.e., specification of meaning of the notation; and pragmatics, i.e., specification of needed actions and rules. The model itself should be easy to understand and expressive. In other words, the model could correctly illustrate the input, and the output should meet the expectations of stakeholders.

By «cost-effectiveness modeling» we mean the cost-effectiveness of the selection of security controls, or in general the security investment. The inputs to the models are based on the results from the decision making method, that is the discovered vulnerabilities, the suggested controls to mitigate risks, and the total cost of implementation sorted based on Cyber Kill Chain (CKC), Cybersecurity Framework (CSF), and Critical Security Controls Top 20 (CSC). The outputs show the correlation between: (1) suggested controls towards CKC steps, (2) vulnerabilities and suggested controls towards total cost of implementation grouped by CSF functions, and (3) vulnerabilities and suggested controls towards total cost of implementation grouped by CSC areas.

1.3. Thesis structure

This proposed thesis is organized into the following chapters:

Chapter 1 - Introduction motivates the needs for a decision making method that supports risk assessment, selection of security controls, and cost-effectiveness analysis. It also presents the research problem, main objective as well as the contribution of this thesis. The thesis structure is also outlined in this chapter.

Chapter 2 - Identifying needs introduces the stakeholders who gain benefits from the presented objective. In addition, this chapter presents a set of pre-defined success criteria that should be carried through our artifacts in order to reach the overall objective.

Chapter 3 - Research method presents a method for technology research and how the method has been utilized throughout this thesis.

Chapter 4 - State of the art presents the relevant state of the art for this thesis.
Chapter 5 - Artifacts provides the overview of developed artifacts, including the checklist for security consultant, the decision making method and the cost-effectiveness models, as well as the way they are used together.

Chapter 6 - Evaluation of artifacts presents the evaluation of developed artifacts throughout a case study.

Chapter 7 - Evaluation with respect to success criteria discusses to what extent the pre-defined success criteria have been fulfilled by our presented artifacts.

Chapter 8 - Threats to validity and reliability addresses difficulties during our research that might have affected the validity and reliability of the thesis.

Chapter 9 - Conclusions and Future work presents conclusions regarding the contribution of this thesis and proposes potential areas of future work.
Chapter 2
Identifying needs

In chapter 1 we presented the research focus, that is the overall motivation through the problem and the objective for our research. In this chapter, we clarify this objective with a set of success criteria and all the parties involved. Sections 2.1 represents the stakeholders involved in the decision making process as well as their roles. In section 2.2, we define the success criteria for each artifacts mentioned in chapter 1. In other words, the fulfillment of each set of success criteria for each artifact is necessary for the accomplishment of our main objective.

2.1. Stakeholders

2.1.1. Security consultants

Security consultants are risk analysts working in the field of Information Security. They are expected to be knowledgeable in a diverse set of technical skills, including risk assessment standards, security frameworks and security controls, and are able to identify risks and vulnerabilities in order to implement risk analysis. Security consultants provide sufficient security controls and treatments, and are able to implement cost-effectiveness modeling. Security consultants collaborate closely with the organizations.

According to our empirical data collected after the launch of the questionnaire, security consultants are interested in these following contributions among others:

- Industry standards & Readily available relevant data
- Knowledge of all the different ways to implement controls
- A well vetted, simple worksheet that can be used across industries and controls
- Visualization tools

Our artifacts, briefly presented in chapter 2, as a result refer back to the needs of security consultants, and therefore should to an extent satisfy what security consultants are looking for. The checklist as well as the tool support should include up-to-date industry standards and
identified needs
guideline for security controls, methods for calculating and/or estimating cost, effect and benefit of controls. Both checklist and tool support should be properly organized, comprehensive for all stakeholders, and contribute to the process of decision making method. Last but not least, the results should be correctly and expressively modeled in the way that it would be easier for security consultants to present the results to organizations.

Security consultants play an important roll in the process of decision making method. They are the one who lead the process, use the checklist and tool support to identify threat agents based on historical data of security events, identify vulnerabilities by running vulnerabilities scan, register risks and select appropriate controls to mitigate risks, estimated cost, effect and benefit of suggested controls, and then model the results.

2.1.2. Decision makers

Decision makers are clients represented by organizations, businesses and enterprises. They usually have limited knowledge within the field of Information Security. Decision makers have to decide what is the asset for their business, and provide security consultants valuable information regarding threats and risks under the risk evaluation process. Decision makers, which are also end-users, will decide whether the solution from security consultants covers their need during the final state of the decision making process, pay for the result, and implement the security controls to reduce risks.

Decision makers are interested in an easier way to get better overview over their own risk picture, a «Good management dashboards with drill-down capabilities» referred back to the questionnaire response. The tool support should therefore able to show how vulnerable the organization is at the time of the implementation of risks assessment and decision making process, how many security controls they need to mitigate risks, and how much will it cost the organization. The models should then be able to illustrate the correlation between vulnerability, controls and cost of implementation.

2.2. Success criteria

In order to achieve the overall research objective, we need to identify and evaluate a set of success criteria. Based on the previous discussion, we now present four artifacts in the first part of this section. Each artifact therefore has its own success criteria that should make the thesis to be succeeded. In the other part of this section, we shall discuss each of these artifacts in terms of form and content. The artifacts we focus on are as following:

- The checklist for security consultants
• The tool support for the decision making method
• The process of decision making method
• The approach to cost-effectiveness modeling

2.2.1. The checklist for security consultants

The checklist for security consultants, conducted based on the experience of domain experts, is used as a guideline for security consultants as well as organizations during the process of decision making method.

The following success criteria have been identified:

SC 1: Comprehensibility of the checklist

The checklist should provide a sufficient and comprehensible list of activities and common understanding for the stakeholders, specially the security consultants who use the checklist actively throughout the decision making process.

SC 2: «Sorting/Grouping» of the checklist

Each point in the checklist should be divided in different groups based on its purpose and arranged in the order of implementation.

2.2.2. The tool support for the decision making method

The tool support is meant to be used together with the checklist that assists the security consultants during the process of decision making method.

The following success criteria have been identified:

SC 3: Accuracy of the tool support

The essential functions should give correct and reliable output according to the input data.

SC 4: Usability of the tool support

The tool should have a graphical user interface which is easy to use and understand for all end-users.

SC 5: Efficiency of the tool support

The tool should be feasible and can be used within allocated resources in a realistic industrial context. Time consumed should also be sufficient.
2.2.3. The process of decision making method

The process of decision making method in the context of our research is designed in order to guide security consultants and organizations to achieve their goal throughout a sequence of actions carried out by certain actors.

The following success criteria have been identified:

SC 6: Comprehensibility of the decision making process

The process should provide a sufficient and comprehensible description of activities and common understanding for the stakeholders, specially the security consultants who manage the whole process and document the results.

SC 7: Correctness of the decision making process

The process should provide reliable advices and measurements. The security consultants should be able to give proper suggested controls based on its cost and effect.

2.2.4. The approach to cost-effectiveness modeling

Based on the security frameworks and security controls, security consultants develop models which provide a common understanding of the organizations’ cost-effective factors. The models are supposed to be adequately understood by the stakeholders.

These following success criteria have been identified:

SC 8: Comprehensibility of the cost-effectiveness models

The models should have clear syntax and semantics, together with adequate illustrating method. The models should also provide a sufficient common understanding to both internal and external stakeholders.

SC 9: Correctness of the cost-effectiveness models

The output from the models should be accurate for the purpose intended. Besides, the models should also provide sufficient understanding of the target system by covering all the aspects defined during the analysis process.

SC 10: Expressiveness of the cost-effectiveness models

The models should provide necessary information needed and the structure of the models should be complete and sufficient.
Chapter 3
Research method

In this chapter, we present the selection of research method implemented throughout this thesis. Section 3.1 briefly introduces three common stages of research method, followed by strategies for evaluation presented in section 3.2. In section 3.3, we discuss why this particular research method is appropriate in the context of this thesis. Section 3.4 and 3.5 present some common methods for collecting empirical data and why some particular methods are chosen. Lastly, we describe how selected research method has been applied in section 3.6.

3.1. Research method

Drawing on the challenges discussed from previous chapters, we briefly consider a research method that would be appropriate for conducting our thesis. Despite the difference between the basic questions leading the classical researcher on the one hand and the technology researcher on the other hand, Solheim and Stølen [15] have claimed that technology research, like classical research, is an iterative process, and can be characterized by the following three main steps as illustrated in figure 3.1:

![Figure 3.1.: Method for technology research (adopted from Solheim and Stølen [15])](image-url)
• **Problem analysis**: The researcher maps a potential need for a new or improved artifact by interacting with possible users and other stakeholders.

• **Innovation**: The researcher attempts to construct an artifact that satisfies the potential need. The overall hypothesis is that the artifact satisfies this need.

• **Evaluation**: The researcher formulates predictions about the artifact and checks whether these predictions come true. If the results are positive, the researcher may argue that the artifact satisfies the need.

### 3.2. Strategies for evaluation

#### 3.2.1. Overview of strategies

There exists a wide range of research methods and each research method has its own strengths and weaknesses. According to McGrath [27], there are three desired properties that should be maximized after gathering research evidence:

- **Generality**: The generalization of results across populations. Various research methods can provide different degree of generalization from a much smaller sample.

- **Precision**: The degree of preciseness in measurements. Accuracy and preciseness in measurements is important to obtain sufficient results.

- **Realism**: The degree of realistic situation or context. A research conducted in a realistic situation is believed to have more accurate results.

A research method that scores highest at all three properties would obviously be the optimal choice. As stated by McGrath [27], using multiple research methods might add strength to the resulting evidence by offsetting each other's weaknesses. In other words, it is impossible to maximize all strengths with just one research method.

McGrath has divided research strategies into four categories, together with some of the most common one:

- **Artificial setting**: Laboratory experiments, Experimental simulations

- **Natural setting**: Field experiment, Field study

- **Independent of empirical evidence**: Computer simulation, Non-empirical evidence

- **Independent of setting**: Qualitative interview, Survey
3.2.2. Case study

One of these most common strategies for evaluation is case study. A case study, as proposed by Yin [31], is an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident. A case study [29] involves an in-depth examination of a single instance – a case. A case study method is, according to Yin [31], used when the researcher deliberately wants to uncover contextual conditions – believing that they might be highly pertinent to the phenomenon of study. A case study [29] comprises an all-encompassing method – covering the logic of design, data collection techniques, and specific approaches to data analysis. One of the common drawbacks with case study is that researchers attempt to answer a question that is too broad or a topic that has too many objectives for one study.

3.3. Selection of evaluation method

Both case study and technology research provide the opportunity to examine ideas and innovative solutions in real-life settings. When considering resource limitations associated with our research, both case study and technology research take into account various resource constraints. Additionally, case study implemented after the Diagnose phase (Problem Analysis) helps us to collect empirical data, then case study can also be used later on to evaluate the desired effect of our findings and result. As illustrated in figure 3.2.1, both case study and technology research provide sufficient degree of generality, precision, and realism. Drawing on the strengths of case study and technology research, we believe that case study and technology research might be appropriate for conducting our research.
3.4. Empirical data collection

Empirical research methods [32] to a large extent is not only about technical solutions, but also concerned with organizational issues, project management and human behavior. In other words, it is a way of gaining knowledge by means of direct and indirect observation or experience [32]. The research method applied in our research paper is an empirical research. That's why there is a need for collecting empirical evidence.

According to Donmez [35], there are four main methods to collect empirical data:

3.4.1. Interview

This is the most widely used method in qualitative research that gives researchers the ability to explore new and complex issues by developing models. However, this method is intensive in term of resources and often influenced by researchers' expertise.

Typically, there are three types of interview [35]:

- **Structured/standardized interview**: the same list of very specific questions to everyone, range of answers may be given.
- **Unstructured interview**: informal style with a list of topics to cover, questions are mostly open.
- **Semi-structured interview**: the list of questions which can be varied, modified or extended during the interview.

3.4.2. Observation

This method is often used in parallel to interviewing. Observation is often intentional and goal-oriented that focuses on specific behaviors since some certain types of data can be collected only by observation (gesture, facial expression, interaction, etc.). The purpose of observation is to describe setting, activities, people and meaning of what was observed.

Some common types of observation [35]: Covert vs. Overt, Participant vs. Non-participant, Structured vs. unstructured observations, Collecting field notes, Avoiding biases.

3.4.3. Questionnaire

This method is a useful and pragmatic way of collecting data, in particular for larges samples. However, the way data is collected can influences the answers. Therefore, good questionnaire design is vital for collecting reliable and valid data.
Some regular types of questionnaires [35]: Performance tests, Personality tests, Self report, Behavior, Opinions.

3.4.4. Literature research

This method is usually performed at the beginning of the project. This can be done by answering some questions like [35]: What is already known about this area of research? What concepts and theories are relevant to this area? What methods have previously been employed? Literature research is a systematic review which can be achieved by using search engines or references from important books or articles.

3.5. Selection of empirical data collection method

As discussed above, the empirical data collection methods should maximize three properties at a desired extend. Indeed, interviews and questionnaires fall into the “Independent of setting” category of research strategy and bring forth the generality property. Besides, qualitative interview with domain experts within the field of Information Security also provide sufficient degree of preciseness in measurements that qualifies the precision feature. Drawing on the strengths discussed above, we believe that these first three methods for empirical data collection: (1) Interview, (2) Observation, and (3) Questionnaire might be appropriate in order to maximize the essential features of generality, precision and realism.

3.6. How we have applied selected research method

As presented earlier, technology research and case study have been chosen to be applied in our research. Regarding the collection of empirical data, these three methods (1) Interview, (2) Observation, and (3) Questionnaire have also been selected. In this section we present how we have applied chosen research method and methods for collecting empirical data in our thesis regarding our artifacts and their predefined success criteria.

Figure 3.6 below illustrates the iterative process that was undergone during the development of the artifacts.
Chapter 3

Research method

Figure 3.6: Research method (adopted from Refsdal [46] and modified)

1. Identify success criteria for artifact
2. Propose artifact
3. Evaluate based on case study
4. Evaluate based on results of questionnaire
5. Evaluate based on observations
6. New insight w.r.t. requirements?
7. Requirements fulfilled?
8. Adopt artifact

Problem Analysis

Innovation

Evaluation

Yes

No
3.6.1. The checklist for security consultants & The tool support

For the purpose of gathering empirical data as input for conducting the checklist for security analysts and the tool support, a questionnaire was created by Google Forms on 25 November 2016 and can be accessed by this link https://goo.gl/forms/oehDDFgj80FZ1vOl2.

The questionnaire is composed of four parts: (1) Introduction and Objective, (2) General questions, (3) Multiple choice questions, and (4) Open questions and comments. Firstly, we briefly introduce our thesis and the main objective of the research in part one. Secondly, we ask domain experts about themselves and their backgrounds in part two. The focus of this questionnaire lays on part three where there are twelve questions ordered by different categories. The main purpose of this part is to gather the latest trend in the market regarding risk assessment and cost-effectiveness analysis. Domain experts can see slightly different set of questions depending on their backgrounds (whether they are IT security consultants or not). Last but not least, we provide two open questions and a comment section in part 4 of this questionnaire in order to understand the needs for a better decision making method.

The questionnaire was sent to a selected group of domain experts on 29 November 2016 and last until the end of the year. We have received 17 responses illustrated by the graph below:

![Responses received sorted by date](image)

For the sake of privacy, including personal and sensitive information, all provided data is processed anonymously and only for the purpose of this research. Moreover, there is no IP tracking and domain experts do not need to register their emails while submitting responses. Detailed information about the questionnaire, collected responses and written feedbacks are presented in Appendix A and Appendix B.

We discuss about the evaluation of the checklist for consultants and the tool support together with the evaluation of the decision making method in the next section.
3.6.2. The process of the decision making method

As mentioned above, the evaluation of the process of the decision making method is conducted mainly based on a case study. Our case study was developed partially based on the intrusion event introduced by Hutchins [48]. In other words, the case is not totally in a real life context since the case is about a fictitious organization and some of the intrusion attempts are not real attacks. However, we tried to keep the case as much realistic as possible. The introduction of the case as well as its background and context will be presented in more detail in chapter 6. Additionally, observations were made during the evaluation of the process.

During the evaluation of the checklist, the tool support and the process of decision making method, their predefined sets of success criteria presented in chapter 2 are also considered. For the checklist, we mainly focus on the comprehensiveness and how all the points are organized and sorted based on its function. Then for the tool support, we for the most part focus on the accuracy, usability and efficiency. Lastly, for the process of the decision making method we primarily focused on the comprehensibility, correctness, and expressiveness of the models. Besides, feedbacks from domain experts collected from the questionnaire are also used as references for evaluation.

3.6.3. The approach to cost-effectiveness models

Similarly to the evaluation of process of the decision making method, the evaluation of the approach to cost-effectiveness models was partially based on the same case study, or more precisely based on the output of the decision making method throughout case study. During the evaluation of the approach to cost-effectiveness models we primarily focused on the comprehensibility, correctness, and expressiveness of the models which reflects their predefined success criteria presented in chapter 2. Feedbacks from domain experts presented in Appendix B are also used as references for evaluation.
Chapter 4
State of the art

In this chapter, we conduct a state of the art with respect to our artifacts mentioned in section 1.2. While section 4.1 presents some industry standards, popular risk analysis approaches are introduced in section 4.2. Later on, section 4.3 characterizes some micro-economics techniques that have been used to justify security expenditure. In section 4.4, the decision theory, the study of making rational and optimal choices, is briefly presented. We also provide a selection of tool support and development environments in the last section of this chapter.

4.1. Risk assessment standards

We now take a closer look to two standards codified by the International Organization for Standardization (ISO), followed by Special Publication by the National Institute of Standards and Technology (NIST) and a good-practice framework proposed by International Professional Association (ISACA).

4.1.1. ISO 27000 family

First of all, the ISO 27000 family of standards helps organizations keep information assets secure. ISO/IEC 27001:2013 [6] is a known standard in the family providing requirements for an Information Security Management System (ISMS). The ISMS preserves the confidentiality, integrity and availability of information by applying a risk management process so that risks are adequately managed. In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved. Moreover, in order to support the general concepts specified in ISO/IEC 27001, ISO/IEC 27005:2011 [7] is designed to assist the satisfactory implementation of Information Security based on a risk management approach.

4.1.2. ISO 31000 family

ISO/IEC 31000 is the second standard among others. The ISO 31000 family provides principles and generic guidelines relating to risk management. ISO/IEC 31000:2009 [8] can be applied throughout the life of an organization, and to a wide range of activities, including
strategies and decisions, operations, processes, functions, projects, products, services and assets. Furthermore, the ISO/IEC 31010:2009 provides guidance on selection and application of systematic techniques for risk assessment that supports ISO 31000:2009 [9].

4.1.3. NIST SP 800-30

Additionally, we also consider the Special Publication 800-30 by NIST. The NIST SP 800-30 [5] is a risk management guide for Information Technology systems. This guide provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems [5]. In addition, this guide also provides information on the selection of cost-effective security controls.

4.2. Risk analysis approaches

According to the Society for Risk Analysis (SRA), risk analysis has been defined in many different ways, and much of the definition depends on how risk analysis relates to other concepts. In this part, we have a focus on some specific approaches that help us to define and thus gain more understanding about threats, vulnerabilities and security controls.

4.2.1. INTEL Threat Agent Library (TAL)

First of all, the unique standardized Threat Agent Library developed by Intel IT guides us to identify potential threats. INTEL [17] has stated that TAL has provided a consistent, up-to-date reference describing threats to IT systems and other information assets. Furthermore, TAL [17] also helps risk analysts identify accurately and understand the importance of relevant threat agents. This library consists of 22 standardized archetypes that represent external and internal threat agents, ranging from industrial spies to untrained employees. As claimed by INTEL, the library is designed to overcome the lack of standard threat agent definitions and the problem that threat information is often fragmented and sensationalized.

According to INTEL, attackers are hostile and start with intent to harm or inappropriately use organization’s assets. Attackers could be mobsters/thieves (part of organized criminal group), competitors, or even internal spies as following:

**Access**

- Internal access or/and External access

**Motivation / Outcome**
• Acquisition/Theft: Financial gain from funds and financial instruments or theft of traded secret/HCI

• Business advantage: Increased ability to compete in the market

• Technical advantage: Increased production process and capability, rather than business process

Limits

• Extra-legal (minor): Attackers might break the law in relatively minor, non/violent ways

• Extra-legal (major): Attackers take no account of the law

Resource

• Individual: Attackers act independently

• Organizational: Attackers operate in multiple geographies and long term

Skill

• None: Attackers have regular skill and ability to perform random acts, rather than required expertise for a targeted attack

• Adept: Attackers are expert in the field, both in technology and attack methods
  • Able to take advantage of publicly announced vulnerabilities before the targeted victims’ systems are fully patched
  • Able to create solid phish from a tiny bit of information
  • Able to create trojan that hardly can be detected
  • Able to take advantage of zero-day-vulnerabilities with complicated (encrypted) attack code

Objective

• Copy: Attackers make a replica of the asset in order to have concurrent access

• Take: Attackers gain control of the asset and the organization doesn't have access

Visibility

• Covert: The attack is discover but attackers remain unidentified
• Clandestine: Both the attack and attackers’ identity remain secret

Behavior

• Attackers pose as a legitimate financial institution from a foreign country

• Attackers take advantage of natural disasters, large public events, holidays, or even massive data breaches to phish large groups of targets for information

• Instead of sending out thousands of e-mails randomly hoping a few victims will bite, attackers target selected groups of people with something in common and usually with high profile

<table>
<thead>
<tr>
<th>Access</th>
<th>Mobster</th>
<th>Thief</th>
<th>Competitor</th>
<th>Internal spy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outcome</td>
<td>External</td>
<td>Internal</td>
<td>External</td>
<td>Internal</td>
</tr>
<tr>
<td>Limits</td>
<td>Extra-legal, major</td>
<td>Extra-legal, minor</td>
<td>Extra-legal, minor</td>
<td>Extra-legal, minor</td>
</tr>
<tr>
<td>Resources</td>
<td>Organization</td>
<td>Individual</td>
<td>Organization</td>
<td>Organization</td>
</tr>
<tr>
<td>Skills</td>
<td>Adept</td>
<td>None</td>
<td>Adept</td>
<td>Adept</td>
</tr>
<tr>
<td>Objective</td>
<td>Take</td>
<td>Take</td>
<td>Copy</td>
<td>Copy</td>
</tr>
<tr>
<td>Visibility</td>
<td>Covert</td>
<td>Clandestine</td>
<td>Clandestine</td>
<td>Clandestine</td>
</tr>
<tr>
<td>Tactic</td>
<td>Thief of IP, PII, or business data</td>
<td>Thief of hardware, IP, PII, or business data</td>
<td>Thief of IP or business data</td>
<td>Thief of IP, PII, or business data</td>
</tr>
</tbody>
</table>

Table 4.2.1: Attackers’ attributes (adapted from INTEL TAL [17])

4.2.2. CORAS and PREDIQT

The next important step is to analyze risks and vulnerabilities that have both negative and positive effects on the defined assets. There are a variety of approaches out there in the market. An approach called CORAS [25], a general model-driven approach to risk analysis, among others, has been applied to a large variety of risk analysis targets and concerns within numerous domains. A risk analysis using CORAS [25] consists of eight steps that comprise every stage from the initial preparations through deriving the eventual results and conclusions. Each step is divided into concrete, practical subtasks with a clearly defined objective as following: (1) Preparations for the analysis, (2) Customer presentation of the target, (3) Refining

PREDIQT [29], a method for model-based prediction of impacts of architectural design changes on system quality, provides understanding of the system design and the alternatives for potential improvements, as well as existing and potential weaknesses of architectural design, with respect to individual quality characteristics and their tradeoffs [25].

4.2.3. Lockheed Martin Cyber Kill Chain (CKC)

In order to investigate the attack chain, we use the so-called Cyber Kill Chain, a methodology adapted to Information Security by Lockheed Martin [47]. They describe seven phases in which all attacks go through in a variant of degrees. This secures that we do a structured analysis of how an attack occurs, seen from the view of attackers. For every phase, we describe what could happen, and connect vulnerabilities toward different phases. Business self must make a choice if something should be done or implemented.

Primarily, these are two attack techniques, via web-browsers and/or email attachments, and they have two different attack vectors to get attack code onto the target’s computer. When attack code is first transmitted, the same vulnerabilities can be exploited. Therefore, the first three phases can be analyzed separately, and the last four together. Here is the seven phases:

1. **Reconnaissance**
   - **Via web-browsers:** Threat Agent examines the organization, sector and websites with geographic relevance (different offices), and creates a list of sites most likely to be visited by employees. This may be news sites, blogs, portals or suppliers websites for tools and systems that are commonly used or are visited by a special group of employees.
   - **Via email attachments:** Threat Agent examines the organization, sector, official and unofficial information necessary to identify key personnel and possible information they want or expect to receive, as well as who they expect to receive this information from.

2. **Weaponization**
   - **Via web-browsers:** Threat Agent tries to find vulnerabilities that can be exploited on relevant websites. If possible, Threat Agent gets web servers compromised. If that's not possible, Threat Agent may attempt to attack the business operating the servers in order to get enough permissions to modify the content of websites. This also applies to sub-contractors of content, such as ads for an online newspaper.
Chapter 4

State of the art

Via email attachments: Threat Agent tries to find vulnerabilities that can be exploited either in the current email client, or other applications or libraries the staff is using, such as Microsoft Office, Adobe Reader, or programs to view images.

(3) Delivery

Via web-browsers: When an employee visits a compromised website, it is sent over attack code tailored to the particular client. Threat Agent may limit the attack to apply only to business IP address range, to limit exposure and the opportunity to be discovered. It can be used «obfuscation techniques», such as XOR, and also encrypted code, to make it difficult for signature-based detection mechanisms to detect code.

Via email attachments: A file with seemingly legitimate content can be sent to a receiver or a list of receivers. The file will contain malware that the attacker wants the user to run. The file may also be in the form of an image or other objects in the body of the email. The encryption technique is the same as above.

(4) Exploitation

To execute attack code, it will often be possible to achieve this without user involvement. If it is a vulnerability related to processing of an object, the object will normally automatically processed, which in turn causes the attack code is executed. If vulnerability requires the user actively starting attack code, this is made possible through tricking the user into thinking that it's relevant information (eg. a PDF file) or a useful tool that installs (eg. Adobe Flash update), but which also contain attack code.

(5) Installation

Assuming that the Threat Agent has managed to acquire permits user rights for installation of software, Threat Agent will now install a Trojan right after attack code is executed, ensuring a backdoor to the system is compromised.

(6) Command & Control (C2)

A compromised machine normally sends out data to provide Threat Agent access to the computer. It then sends the data to the predefined command and control servers, to establish a session with these and give Threat Agent direct control over the compromised computer. The traffic is often encrypted, either directly via SSL or indirectly in other communications.
(7) Actions on Object

When Threat Agent has complete control of the compromised machine, the goal of compromising is accomplished. For this targeted attack, it is assumed that the goal is to obtain a foot inside the company’s network, and use this access to attack other systems, which is the primary objective of Threat Agent.

![Cyber Kill Chain](adopted from Lockheed Martin [47])

4.2.4. NIST Cybersecurity Framework (CSF)

With the same ambition, it is essential to figure out what kind of security controls the clients have in place, as well as controls they are missing that open the door for vulnerabilities. For that purpose, Cybersecurity Framework (CSF) has been introduced. As stated by NIST [4], the CFS has a prioritized, flexible, repeatable, and cost-effective approach. Besides managing cybersecurity-related risk, the CSF [4] also endorses the protection of critical infrastructure both
for owners and operators. The CSF focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. In other words, the CSF provides a common mechanism for the clients to describe their current disposition and target state, identify continuous and repeatable process, assess toward the target state, as well as to communicate among internal and external stakeholders.

Arcading to NIST, the framework is composed of five main functions: (1) Identify, (2) Protect, (3) Detect, (4) Respond, and (5) Recover. Firstly, «Identity» function helps organization to understand and manage cybersecurity risks in order to protect their systems, assets, data, and capabilities. Secondly, «Protect» function assists organization to limit the impact of attacks by implementing sufficient security controls. Thirdly, «Detect» function lets organization develop suitable activities to discover the occurrence of a cybersecurity event, followed by «Respond» function that supports organization with appropriate actions when cybersecurity events encounter. Lastly, «Recover» function helps organization with proper activities to get back to normal operations and reduce the impact due to cybersecurity events. Main outcomes of each CSF function are illustrated in the table below:

<table>
<thead>
<tr>
<th>IDENTIFY</th>
<th>PROTECT</th>
<th>DETECT</th>
<th>RESPONSE</th>
<th>RESTORE</th>
</tr>
</thead>
</table>
| • Asset management  
• Business environment  
• Governance  
• Risk assessment  
• Risk management strategy | • Access control  
• Awareness and training  
• Data security  
• Info protection and procedures  
• Maintenance  
• Protective technology | • Anomalies and events  
• Security continuous monitoring  
• Detection process | • Response planning  
• Communicatio n  
• Analysis  
• Mitigations  
• Improvements | • Recovery planning  
• Improvements  
• Communicatio n |

Table 2.1: Cybersecurity Framework Core Outcome (adopted from NIST [4])

4.2.5. CIS Critical Security Controls (CSC)

Last but not least, CIS Top 20 Critical Security Controls (CSC) [11], among others, have also provided a list of security guidances in priority order that help security consultants identify the Minimum Security Requirements (MSR) as well as the missing controls. The CSC focuses on prioritizing security functions that are effective against the latest Advanced Targeted Threats. Indeed, the Controls do not attempt to replace the work of CIS, including the CSF or SP 800-53 discussed above. The Controls instead prioritize and focus on a smaller number of actionable controls with high-payoff, aiming for a "must do first" philosophy.

The list below gives us the overview of CIS Critical Security Controls Top 20:

- CSC 1 - Inventory of Authorized and Unauthorized Devices
Chapter 4
State of the art

- CSC 2 - Inventory of Authorized and Unauthorized Software
- CSC 3 - Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- CSC 4 - Continuous Vulnerability Assessment and Remediation
- CSC 5 - Controlled Use of Administrative Privileges
- CSC 6 - Maintenance, Monitoring, and Analysis of Audit Logs
- CSC 7 - Email and Web Browser Protections
- CSC 8 - Malware Defenses
- CSC 9 - Limitation and Control of Network Ports, Protocols, and Services
- CSC 10 - Data Recovery Capability
- CSC 11 - Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- CSC 12 - Boundary Defense
- CSC 13 - Data Protection
- CSC 14 - Controlled Access Based on the Need to Know
- CSC 15 - Wireless Access Control
- CSC 16 - Account Monitoring and Control
- CSC 17 - Security Skills Assessment and Appropriate Training to Fill Gaps
- CSC 18 - Application Software Security
- CSC 19 - Incident Response and Management
- CSC 20 - Penetration Tests and Red Team Exercises

4.3. Microeconomics models

The importance of effective management of Information Security has increased in recent years due to increasing frequency and cost of security breaches [19]. According to the Computer Crime and Security Survey [28], much of the industry has begun to embrace the economic metrics to validate the security department expenditures by expressing them in terms of Return on Security Investment (ROSI), Net Present Value (NPV) and Internal Rate of Return (IRR).

Firstly, the ROSI [19] states the non-financial and financial benefits of Information Security or an Information Security initiative compared to its costs. The main purpose for using ROSI is to
justify the security project budget and to provide common directions for IS management [19]. 

ROSI refers to the calculation of the financial return from an investment in security based on the financial benefits and costs of that investment. We can express ROSI in this term:

\[
\frac{(\text{what} - \text{I} - \text{gained - totally}) - (\text{what} - \text{I} - \text{invested})}{(\text{what} - \text{I} - \text{invested})}
\]

Equation 4.3.1: Return on Security Investment (adopted from Su X. [19])

Starting with the idea of ROSI, several concepts have been developed to support the decision for or against an information measure. One way to do this is to apply the concept of NPV [20]. The following model returns a positive or negative value, and an organization thus decides whether to make a security investment or not based on that output:

\[
NVP = -I_0 + \sum_{t=1}^{T} \frac{\Delta E(L_t) + \Delta OCC_t - C_t}{(1 + i_{calc})^t}
\]

\[I_0= \text{initial investment for security measure}\]
\[\Delta E(L_t)= \text{reduction in expected loss in } t\]
\[\Delta OCC_t= \text{reduction in opportunity costs in } t\]
\[C_t= \text{cost of security measure in } t\]
\[i_{calc}= \text{discount rate}\]

Equation 4.3.2: Net Present Value (adopted from Brecht and Nowey [20])

Lastly, the IRR [20] is an economic metric discussed that a security manager might use to evaluate a project expenditure. The IRR is calculated by using a cash flow like NPV. Brecht and Nowey [20] agree that IRR, unlike the NPV calculation, shows a security manager at what rate we break even.

4.4. Decision theory

So far we have been considering risk assessment standards - general knowledge required - in section 4.1, then our main focus: risk analysis approaches - what to do for security consultants - in section 4.2, followed by section 4.3 with some microeconomics models. The result from all the discussions above is a list of solutions that clients choose from. We can see from here that there are a lots of crucial and complex decisions to make in association with risk, security controls and cost-effectiveness. For security consultants, it is about how to classify different security controls and decide optimal investment for each security function. For clients, it is about how to choose a sufficient solution based on their own security strategy and risk aversion that could gain them a cost-effective improvement for the whole system. As a
consequence, decision theory has been used to provide support for selection since it is essential for both security consultants and their clients since there are often a lot of major and complex decisions to be made during the cost-benefit analysis process.

Decision theory [43] is theory about decisions concerned with goal-directed behavior in the presence of options. In other words, decision theory [43], or theory of choice, is concerned with identifying the values, uncertainties and its rationality that results an optimal decision. There are two types of decision theory: normative and descriptive. Normative, or prescriptive, decision theory [43] is a theory about how decisions should be made, that is to identify the best decision to take. In contrast, descriptive, or positive, decision theory [43] is a theory about how decisions are actually made, concerned with describing observed behaviors under the assumption that the decision-making agents are behaving under some consistent rules.

As mentioned above, the decisions are complex since there are often a large number of different factors that must be taken into account when making the decision, especially when uncertainty involved. Furthermore, a decision maker’s attitude toward risk taking can also have relative great impact on different decision alternatives. That is what we call risk aversion. According to Keeney [42], there are three types of risk aversion associated with utility function. For the first one, a decision maker is a risk averse if and only if his utility function is concave [42]. Secondly, a decision maker is a risk seeking if and only if his utility function is convex [42]. Lastly, if a decision maker is neither risk averse nor risk seeker, then he is risk neutral and is indifferent between choices.

![Risk aversion illustrated by Utility function](adopted from Policonomics [37])

There are a variety of decision support tools out there in the market that have been used in order to address such complexity. Among them, decision tree [44], a diagram of solution, provides a convenient and efficient representation of knowledge by using a tree-logic to make predictions. According to Ledolter [44], in a decision tree, each decision defines a node while
the final prediction is made at a leaf node, and the leftmost node in a decision tree is called the root node. He also declares that a decision tree consists of 3 types of nodes: (1) decision nodes - commonly represented by squares, (2) chance nodes - represented by circles, and (3) end nodes - represented by triangles.

4.5. Tool support & Development environments

The idea of implementing the support tool is to visualize the result of the decision-making process in relation to risk estimation, security controls and cost-effectiveness. The tool also shows the overlap between different security control combinations and pricing in the way that it helps end-users to understand how to make sufficient IT investment.

The support tool should qualify these requirements as following:

- Gathering data (empirical)
- Analyzing and interpreting data
- Visualizing data with graphical illustrations (different kinds of graphs and charts)

There are some possible options regarding the implementation of our tool support:

4.5.1. Excel spreadsheets

- Development environment: Microsoft Excel
- Widespread popularity in academia
- Featuring calculation, graphing tools, pivot tables, and a macro programming language called Visual Basic for Applications (VBA)

4.5.2. RSA Archer

- Development environment: GRC Platform
- Leader in 2017 Magic Quadrant for IT Risk Management Solutions according to Gartner report\(^1\).

As stated by EMC\(^2\) \[34\], RSA Archer provides these following features:

- **Flexible**: users can automate processes, streamline, workflow, access control

• **Unified**: common platform to manage policies, controls, risks, assessments

• **Collaborative**: cross-functional collaboration and alignment that enables users from different background and domains to work together

• **Efficient**: a variety of components provided that helps users model business processes in a fraction of time (in comparison to traditional implementation)

### 4.5.3. CORAS tool

• Development environment: Eclipse (Java based)

• Support on-the-fly modeling using all kinds of CORAS [25] diagrams

### 4.5.4. GNU Octave

• Development environment: Octave (C based)

• High-level programming language, primarily intended for numerical computations

• Widespread popularity in academia and industry

• Open-source with GNU [40] General Public License, mostly compatible with MATLAB
Chapter 5
Artifacts

In this chapter we provide an overview of our main artifacts and explain how they relate to each other. Section 5.1 introduces how we collect data from domain experts and then conduct the checklist for security consultants, followed by section 5.2 where we present the tool support based on the checklist. In section 5.3 we explain how the checklist, all of its involved phases, should be used together with the tool support during the decision making process. The results of this process are used as input for the approach to cost-effectiveness modeling described in section 5.4.

The figure below shows the relationship between our artifacts. Firstly, we need to conduct the checklist for security consultants, then use the checklist as input for the development of tool support. Both checklist and tool support then in further state are used to support the process of decision making method. Lastly, the results that security consultants get from this process are illustrated by the cost-effectiveness models. Moreover, cost-effectiveness models are intended to organizations while they decide which security controls to implement.
5.1. The checklist for security consultants

The checklist for security consultants is meant to be used as a «remember list» that guides security consultants through the decision making process. This checklist is divided into three main groups: (1) Identifying, (2) Estimating, and (3) Selecting where each group contains a set of bullet points. The group name expresses the function of all bullet points in that group. Each point could be a standard, a guideline, an economic formula, etc.

5.1.1. Identifying

Identifying is the first group of the checklist. The purpose of all points in this group is aimed to help security consultants and organizations to identify: (a) their own needs, (b) who could be the attackers, (c) existing and potential risks, and (d) possible security controls that could mitigate risks with the assistant from security consultants. Here is the list:

(a) Identify organization’s need

- Define stakeholders
- Define and prioritize assets and their value
- Define risk tolerance / risk matrix

(b) Identify threat agent

- Threat Agent Library (TAL) from INTEL

(c) Identify risk

- Perform Gap analysis
- Perform risk assessment (e.g. Bowtie, Root cause)
- Perform vulnerability scan for all systems
- Perform continuous monitoring
- Perform log analysis to find possible intrusion patterns based on e.g. signature
- Perform compliance check for all processes and internal policies based on e.g. ISO 27001, Key Risk Indicator (KRI)

(d) Identify security controls

- Brainstorming / Workshop
- Historical/empirical data
• Advice from domain experts
• Based on Confidentiality - Integrity - Availability (CIA) principle
• Based on one or different international industry standards (e.g. ISO 27000 family)
• Based on ISACA Control Objectives for Information and Related Technologies (COBIT 5)
• Based on COSO Enterprise Risk Management Framework
• Based on CIS Critical Security Controls (CSC) Top 20
• Based on NIST Cybersecurity Framework (CSF)
• Based on Lockheed Martin Cyber Kill Chain (CKC)
• Based on NIST 800-83
• Based on ISF Standard for Good Practice
• Based on Open Security Architecture

5.1.2. Estimating

Estimating is the second group of the checklist. All points in this group are developed in the purpose to help security consultants and organizations to estimate: (1) the cost of security controls implementation, (2) the effect of implemented security controls, and (3) the benefit of implemented security controls that in later stage used as input for the selection of security controls. Here is the list:

(a) Estimate cost of security controls implementation

• Estimate provided by domain experts based on previous similar projects
• Calculate the net bypass rate for suggested security controls (e.g. 100% bypass rate means the security control is not effective at all)
• Calculate the total of actual damage for each incident type (baseline scenario)
• Calculate Risk-based Return On Investment (ROI)
• Calculate Net Present Value (NPV)
• Calculate direct costs (costs for tools, consulting, etc.) and indirect costs (costs for operation, awareness training, etc.)

(b) Estimate effect of suggested security controls
- Run questionnaire to estimate Key Performance Indicators (KPIs)
- Base on subjective estimate from domain experts based on similar projects
- Test with use case or real experiment
- Compare with industry statistics and/or market data

(c) Estimate benefit of suggested security controls

- Estimate potential loss per risk and calculate Single Loss Expectancy (SLE)
- Calculate Annual Loss Expectancy (ALE) and compare with final cost of implemented security controls
- Real Option Analysis (ROA)

5.1.3. Selecting

Selecting is the last group of the checklist. The intension of all the points in this group is to assist organizations to sufficiently select one or a set of security controls in order to strengthen their own security baseline. Here is the list:

Select security controls

- Baseline security approach
- Based on cost-benefit analysis
- Based on decision theory
- Based on personal experience or advice from domain expert
- Based on the effect of risk incidents on organization's assets
- Low hanging fruits (Quick wins) / "Gut feeling"

5.2. The tool support for the decision making method

Section 4.5 presented some development environments that have been considered for the purpose of this thesis. To the best of our knowledge within this area, Microsoft Excel and RSA Archer have been taking to the final list for consideration. Both development environments are widely used (specially in the USA for the case of Archer) with many powerful functions. However, due to the fact that we want to make this tool to be an open source solution, that is not involving license issue, and there is no complex «access control» required at this stage of the research, Excel has been chosen over Archer. Later in this chapter we discuss about the design and components of the tool support as well as how the tool support should be used.
5.2.1. The design and components of the tool support

As discussed above, the tool support called «The checklist implementation» has been developed using Microsoft Excel. The design idea is to make this tool support as simple as possible but still fulfills our pre-defined requirements. The tool support is divided into four sections: (1) General information, (2) Metadata, (3) Analysis, and (4) Overall picture as illustrated by the figure below.

![Figure 5.2.1a: The tool support components](image)

(1) General information

This section gives us some essential information about the assessment including the name of the assessment, its target/scope and description, together with planned and actual start/end date. In this section, organizations can also define the owner and manager of this assessment as well as the relevant stakeholders.

According to our checklist for security consultants, this is the first point from Identifying - (1) Identify organization’s need.

<table>
<thead>
<tr>
<th>General Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assessment Name</strong></td>
</tr>
<tr>
<td><strong>Assessment Owner</strong></td>
</tr>
<tr>
<td><strong>Assessment Manager</strong></td>
</tr>
<tr>
<td><strong>Assessment Status</strong></td>
</tr>
<tr>
<td><strong>Other stakeholders</strong></td>
</tr>
<tr>
<td><strong>Target / Scope</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

![Figure 5.2.1b: General Information](image)
(2) Metadata

Based on the responses from our questionnaire (specially verbal feedback), one kind of uncertainties domain experts have to face while implementing risk assessment is whether they have forgotten «something». It could be a step of a phase, a statement from an industry standard, or a possible control to reduce risk. Therefor they look for a kind of «remember list» that remind them what they have done, what to do next, and what should be consider for each phase of the process. Our «metadata library» has been created to serve that purpose.

For the sake of evaluating the decision making method throughout our case study, we have collected and created our metadata with these following industry standards and guidelines:

- **ISO 27001:2013**: Area - Section - Statement
- **SANS Incident Scenarios**: Description
- **Lockheed Martin Cyber Kill Chain (CKC)**: Phase - Description
- **NIST Cybersecurity Framework (CSF)**: Function - Category - Category Description - Subcategory - Mapping to ISO 27001 and CSC
- **CIS Top 20 Critical Security Controls (CSC)**: Control Area - Family - Area Description - Control - Control Description - Mapping to CSC and CKC

According to our checklist for security consultants, this corresponds to Identifying - (4) Identify security controls.

(3) Analysis

This section is considered to be the main and most important element of this tool support. «Analysis» is composed of five main parts: (i) Asset Register, (ii) Threat Agent Register, (iii) Vulnerability Register, (iv) Risk Register, and (v) Remediation Plan.

(i) **Asset Register**: Type - CIA Requirement - Personal Information - Owner - Value - Cost of consequence (figure 5.2.1.c)

(ii) **Threat Agent Register**: Intent - Type (figure 5.2.1.d)

(iii) **Vulnerability Register**: Description - Likelihood - Severity (figure 5.2.1.e)

(iv) **Risk Register**: Description - Threat Agent - Asset - Incident Scenario - Vulnerability - Severity - Consequence - Existing controls (figure 5.2.1.f)
(v) **Remediation Plan**: Risk - Suggested controls - Estimated cost - Expected effect - Expected benefit - Responsible - Planned start date - Planned finish date - Status (figure 5.2.1.g)

<table>
<thead>
<tr>
<th>Type</th>
<th>CIA Trait Requirement</th>
<th>Personal Information</th>
<th>Owner</th>
<th>Value</th>
<th>Cost of Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Confidentiality</td>
<td>Integrity</td>
<td>Availability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 5.2.1c: Asset Register

![Asset Register](image)

![Figure 5.2.1d: Threat Agent Register](image)

![Vulnerability Register](image)
According to our checklist for security consultants:

- Part (i) corresponds to the second point of **Identifying** - (1) *Identify organization’s need*

- Part (ii) corresponds to **Identifying** - (2) *Identify threat agent*

- Part (iii) corresponds to **Identifying** - (3) *Identify risk*

- Part (iv) corresponds to **Identifying** - (3) *Identify risk*

- Part (v) corresponds to **Estimating** - *Estimate cost / effect / benefit of security controls* and **Selecting** - *Selecting security controls*

As illustrated by figure 5.2.1a, the two-ways arrow between section (2) and (3) indicates that the metadata and the analysis support each other in the way that security consultants use information from the «metadata library» to implement the analysis. If there is something missing or should be adjusted, security consultants then update the «metadata library» according to all changes observed.
(4) Overall picture

The output of section (3) is used as input for section (4) where the decision making process results are visualized. The whole process then starts all over again as security consultants can make a copy this tool support, the Excel spreadsheet, and use it as a template for the upcoming assessment. This process is illustrated by the dotted arrow from section (4) to section (1).

5.2.2. How to use the tool

As mentioned above, the tool support is meant to be used as a template, and information from completed assessments can be archived as historical data for further use regarding risk trend and cost-benefit estimation. In other words, every time security consultants begin with a new risk assessment to support the decision making method, they can first make a copy of the tool support «template» and then start filling information from their findings and estimations.

All the spreadsheets in our tool support have been ordered in the way that security consultants start from the very first spreadsheet called «Info», through the «Metadata» section, then one spreadsheet after another until they reach the last spreadsheet called «Remediation Plan». Metadata section has been filed with relevant and updated industry standards and guidelines in advanced so there is no alternation needed unless there is any changes with existing or need for new industry standards or guidelines. Moreover, the metadata also includes mapping across guidelines and standard. At this stage, the results are ready for further evaluation where security consultants work closely with organization and help them to find the most appropriate possible solution.

5.3. The process of decision making method

In this section, we present an overview of the decision making method process. Figure 5.3 below illustrates our process from input to output, including our three main groups from the checklist and four sections from the tool support.

This process has been developed considering the difficulties both security consultants and organizations have to face in order to achieve a proper and cost-beneficial investment in security controls. In other words, our process of decision making method aims to facilitate and systematically guide security consultants throughout the conduct of risk assessment and then bring the results further to the «Selecting» stage where security consultants work closely with organizations to in order to reach our common goal.
Chapter 5

Artifacts

Figure 5.3: The process of decision making method overview

INPUT
- Checklist
- Tool support (w/ Metadata)

IDENTIFYING
- General Information (w/ Stakeholders)
  - (3-i) Asset Register (Type - Value)
  - (3-ii) Threat Agent Register (Intent - Type)
  - (3-iii) Vulnerability Register (Likelihood - Severity)
  - (3-iv) Risk Register (Severity - Consequence - Existing controls)

ESTIMATING
- Remediation Plan (Suggested controls - Estimated cost - Expected effect - Expected benefit)

SELECTING
- Informed decisions

OUTPUT

(1) ISO 27001:2013
- Incident Scenarios
- Cyber Kill Chain
- Cybersecurity Framework
- Critical Controls Top 20 etc.

(2) etc.
5.3.1. The overview of the process

Security consultants are the one who use this process most actively and closely with organizations in order to achieve the desired goal. Before starting the process, there are some requirements that need to be fulfilled beforehand as following:

For organization

- Clearly define their overall objective and vision
- Clearly define the assets and its value
- Clearly define involved stakeholders
- Define the budget and timeframe for implementation
- Prepare supported information such as related processes, compliance requirements, log (historical) data if available

For security consultants

- Carefully read through supported documents received from organization
- Read through and update the checklist (if required)
- Prepare the tool support and update the metadata (if required)
- Run vulnerability scan for all systems together with security analysts

As mentioned earlier, our process of decision making method has been developed based on our checklist and tool support. Therefore, the description for each phase in this process is corresponded to each group in the checklist and each section in the tool support presented in earlier sections of this chapter.

Table 5.3.1 describes the process of the decision making method in detail with important steps, together with relevant input and output for each phase.

5.3.2. How the checklist and tool support are used in this process

The checklist for security consultants and the tool support have been tightly embedded into the process of decision making method. Security consultants and organizations follow this process, from start to end. For each step, there is a corresponding spreadsheet in our tool support where security consultants and/or organizations can use to fill out information as
presented in section 5.2.2. The checklist itself can always be used as a guide throughout this process.

<table>
<thead>
<tr>
<th>Checklist</th>
<th>Tool support</th>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifying</td>
<td>(1) General Information</td>
<td>- Information from organizations</td>
<td>- Defined stakeholders</td>
</tr>
<tr>
<td></td>
<td>(3-i) Asset Register</td>
<td>- Information from organizations</td>
<td>- Defined assets list</td>
</tr>
<tr>
<td></td>
<td>(3-ii) Threat Agent Register</td>
<td>- Information from organizations - Log data (if available)</td>
<td>- Defined Threat Agents list</td>
</tr>
<tr>
<td></td>
<td>(3-iii) Vulnerability Register</td>
<td>- Information from organizations - Results from vulnerability scanning</td>
<td>- Defined vulnerabilities list</td>
</tr>
<tr>
<td></td>
<td>(3-iv) Risk Register</td>
<td>- Information from organizations - Assets list - Threat Agents list - Vulnerabilities list</td>
<td>- Defined risks list - Existing controls</td>
</tr>
<tr>
<td>Estimating</td>
<td>(3-v) Remediation Plan</td>
<td>- Risks list</td>
<td>- Suggested controls - Estimated cost of suggested controls - Expected effect/benefit of controls</td>
</tr>
<tr>
<td></td>
<td>(4) Cost-effectiveness Models</td>
<td>- Vulnerabilities list - Suggested controls - Estimated cost</td>
<td>- Cost-effectiveness models</td>
</tr>
<tr>
<td>Selecting</td>
<td>(4) Cost-effectiveness Models</td>
<td>- Cost-effectiveness models</td>
<td>- List of controls to be implemented</td>
</tr>
</tbody>
</table>

Table 5.3.1: The overview of the process

5.4. The approach to cost-effectiveness modeling

The approach to cost-effectiveness modeling aims to provide security consultants as well as organization a comprehensive support during the decision making process. The first cost-effectiveness model we develop in this section is based on Cyber Kill Chain (CKC) showing the relation between the cost of a control and the effect of stopping an attack as early as possible to minimize the cost of consequence. The other two models, based on Cybersecurity Framework (CSF) and Critical Security Controls Top 20 (CSC), are in form of graphs that visualize the results from the decision making method.
5.4.1. Cost-effectiveness model based on Cyber Kill Chain

Our first cost-effectiveness model is developed based on the Cyber Kill Chain analysis. As illustrated in figure 5.4.1, the model describes the life circle of an intrusion attack. We have three main factors involved in this process: (1) Attackers, (2) Organization, and (3) Controls.

![Figure 5.4.1: Cost-effectiveness model based on CKS](image-url)
Firstly, attackers are the one who have the intension to harm one or many targeted organizations. With Threat Agent Library mentioned earlier, we can to an extent figure out who the attackers are, their skills, and motivation whether it is for financial purpose or just to make a detrimental effect on the organization's reputation. Secondly, it is the organizations who have been targeted and could suffer from the damage of the attacks. This relation is illustrated by the purple arrow. Organizations, of course, have a number of assets they want to protect, and a budget they can invest in security controls in order to strengthen their security baseline as well as be able to protect their assets. That brings us to the third factor here in this model which is controls, or more precisely «security controls». The relationship between organizations and security controls have been shown by the two-ways blue arrow in figure 5.4.1. For each control, there are two things we consider: cost and effect that together give us the general benefit by implementing that control. Lastly, the red arrow closes our life circle of an intrusion attack model by indicating the action that security controls help to stop, fully or partially, the attackers from harming organization's assets.

By adopting the Cyber Kill Chain analysis in our model, we can illustrate how our three main factors relate to the chain. As introduced in section 4.2, when attackers begin to attack organizations, they go through, but not necessarily, all seven steps of the kill chain. The job of security consultants is to figure out what kind of security controls can be applied for a specific organization that help to stop the attack, and not least at which step of the kill chain. The arrows go from «Controls» to the kill chain imply there is at least a control that can fully or partially stop the attack at a particular step. That means the relation between security controls and each step of the kill chain is not one to one (1:1), but many to many (n:n) in the way that one control could stop the attack at many steps, or there are a number of controls should be implemented in order to stop the attack at that specific step. This relation is based on the complexity of the attack itself. Moreover, this relation also indicates that the sooner a control could stop the attack at a certain step, the more effect that control gives. We illustrate this matter by the «Effect Score» (ES) in green. The higher the score is, the more cost of consequence after a successful attack organization can reduce.

5.4.2. Cost-effectiveness model based on Cybersecurity Framework

Our second model includes two graphs that relate to each other as shown in figure 5.4.2. These two graphs are in fact a visualization form of the data from table 5.4.2 (Note: The data in this table is just demo data, not from our case study). As we can see here, all registered vulnerabilities, which are already mapped to security controls, are classified into the five core areas from Cybersecurity Framework based on its severity rating, and counted. We assume
that one vulnerability is mapped to one control. The last column shows the total cost of implementation for all controls in that specific CSF area.

<table>
<thead>
<tr>
<th>Vulnerabilities per CSF</th>
<th>Info</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
<th>Critical</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>0</td>
<td>0</td>
<td>7</td>
<td>7</td>
<td>0</td>
<td>$ 6,000</td>
</tr>
<tr>
<td>Protect</td>
<td>0</td>
<td>11</td>
<td>10</td>
<td>9</td>
<td>0</td>
<td>$ 30,000</td>
</tr>
<tr>
<td>Detect</td>
<td>0</td>
<td>1</td>
<td>7</td>
<td>2</td>
<td>0</td>
<td>$ 3,000</td>
</tr>
<tr>
<td>Respond</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>$ 7,000</td>
</tr>
<tr>
<td>Recover</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>$ 4,000</td>
</tr>
<tr>
<td>TOTAL</td>
<td>0</td>
<td>14</td>
<td>26</td>
<td>23</td>
<td>0</td>
<td>$ 50,000</td>
</tr>
</tbody>
</table>

Table 5.4.2: Cost-effectiveness data based on CSF (Demo data)

Back to our model, the graph to the left shows us which area of the CFS the organization is most vulnerable corresponding to the number of vulnerabilities found. The blue columns from the graph to the right again indicates how each area of the CSF needs to be strengthen by the number of controls required to be implemented, while the green line points out the total implementation cost (mostly direct cost) for each area. For example, the right graph shows that we can improve «Identify» area around four times more than «Respond» area with almost the same cost, or improve «Protect» area around two times more than «Identify» area but the cost is five times higher.

5.4.3. Cost–effectiveness model based on Critical Security Controls Top 20

The last model we develop is quite similar to the one we discussed in section 5.4.2 above, but this time the model is based on Critical Security Controls Top 20. All registered vulnerabilities
are now categorized into each CSC and counted. The table 5.4.3 contains the demo data and the figure 5.4.3 visualizes the data.

<table>
<thead>
<tr>
<th>Vulnerabilities per CSC</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Info</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Critical</td>
<td>Cost</td>
</tr>
<tr>
<td>CSC 1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>$0</td>
</tr>
<tr>
<td>CSC 2</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>$5,000</td>
</tr>
<tr>
<td>CSC 3</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>$3,500</td>
</tr>
<tr>
<td>CSC 4</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>$3,000</td>
</tr>
<tr>
<td>CSC 5</td>
<td>0</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>$2,500</td>
</tr>
<tr>
<td>CSC 6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>$6,000</td>
</tr>
<tr>
<td>CSC 7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>$0</td>
</tr>
<tr>
<td>CSC 8</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>$2,700</td>
</tr>
<tr>
<td>CSC 9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>$3,100</td>
</tr>
<tr>
<td>CSC 10</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>$1,800</td>
</tr>
<tr>
<td>CSC 11</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>$4,000</td>
</tr>
<tr>
<td>CSC 12</td>
<td>0</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>$500</td>
</tr>
<tr>
<td>CSC 13</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>2</td>
<td>0</td>
<td>$2,100</td>
</tr>
<tr>
<td>CSC 14</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>$1,400</td>
</tr>
<tr>
<td>CSC 15</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>$4,450</td>
</tr>
<tr>
<td>CSC 16</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>$3,200</td>
</tr>
<tr>
<td>CSC 17</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>$5,300</td>
</tr>
<tr>
<td>CSC 18</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>$0</td>
</tr>
<tr>
<td>CSC 19</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>$350</td>
</tr>
<tr>
<td>CSC 20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>7</td>
<td>0</td>
<td>$1,100</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td>0</td>
<td>14</td>
<td>26</td>
<td>23</td>
<td>0</td>
<td>$50,000</td>
</tr>
</tbody>
</table>

Table 5.4.3: Cost-effectiveness data based on CSC (Demo data)

Much the same as our model in section 5.4.2, this model also consists of two graph where the first one shows the total number of vulnerabilities for each CSC area, while the second one shows the amount of controls needed as well as the total cost of implementation for each CSC area. An example here is CSC area 6 contains just one control, but this control has the highest cost of implementation, while it is much cheaper to get all controls in CSC area 13 implemented with just one-third the price.
Chapter 6
Evaluation of artifacts

In order to evaluate our artifacts regarding the checklist for security consultants, the tool support, and the decision making method, a case study was developed. In this chapter, we first present a brief description of the case, followed by the evaluation of our artifacts in detail.

6.1. Case description

In this section we first briefly present a fictitious organization created for the purpose of this case, followed by a short introduction about a fictitious case, its background and context. The case was developed partially based on the intrusion event introduced by Hutchins [48]. Lastly, we talk about the two intrusion attempts that organization had experienced.

6.1.1. The organization

The organization is called Perseus ASA. This organization is a medium size company located in Oslo, Norway with about 250 employees. The organization is working mainly in the banking and other financial services industry for over 20 years. Here are the main stakeholders in this organization: Management, local employees, IT group, partners, and customers.

6.1.2. The case background

Using a technique called «News jacking»¹, Threat Agent's choice was widely popular media topics. The new iPhone from Apple Inc (USA) was a phishing email theme. Threat Agent crafted a variety of phishing emails appealing to people's curiosity about the new iPhone. A popular subject line was «Apple's new iPhone: Live Updates». These emails contained links to compromised external websites and are sent in mass. The web links contained various iPhone news, redirected business users to legitimate websites that had been compromised or injected with malicious codes. Threat Agent had hidden the codes to maintain the compromised codes safe for reputation check and web security defense. Threat Agent then installed a Trojan on

user's computer, and thus gained access to the internal network with the rights the user of the machine. Threat Agent now could accomplish other legal attacks, like getting more privileges on the compromised computer or accessing other systems.

«Targeted\(^2\) malicious email» (TME), or spear phishing, is another kind of attack technique which is more complex and requires a certain level of expertise and resources. Threat Agent examines specific organization to find key personnel, then attaches a seemingly legitimate file to an email, e.g., a PDF report or a PPT presentation, which exploits a vulnerability on the client machine when the file is opened or displayed automatically in email reader. The rest of the attack chain is the same as in «New jacking».

6.1.3. The context

The organization had experienced two attack attempts towards Management. They were struggling with the fact that Threat Agent harmed their assets. Precisely, Threat Agent was able to extract personal identifiable information (PII) of employees from their infected systems, and more importantly sensitive data of the organization, i.e., highly confidential information, throughout phishing attack via email attachments and web browsers. Unfortunately, the organization just only used one antivirus program and inline firewall, and no other kind of security controls that filter out malicious traffic. In other words, an attack could not be recognized until the impact of the attack was visible that leads to serious consequences for the organization's assets.

The organization had agreed to spend a certain amount of money to improve their security situation. Their main goal was to be able to identify attack as soon as it begins since the earlier an attack is spotted, the easier it can be stopped. In this way, it would cost the company less to recover from attacks. However, the organization was quite skeptical with the effect that they could gain by implementing security controls as well as how to select the right controls.

6.1.4. The risk picture

**Intrusion attempt 1** (on June 9\(^{th}\), 2008)

- This is a «News jacking» attack toward many employees at the organization. The email claimed to be from a legit individual, and contained a link that forwarded the user to a compromised website.

- The Threat Agent tried to exploit the vulnerability in Java Runtime Environment (JRE) (CVE-2008-5353) that was not announced until 05.12.2008.

Chapter 6
Evaluation of artifacts

- The encrypted attack code was sent over to the client. Once decrypted, the backdoor components was extracted. When active, it would send data to the C2 server 202.abc.xyz.7 via valid HTTP requests.

- Email header:

```
Received: (qmail 58365 invoked by uid 60001); Fri, 09 Jun 2008 22:41:17 +0000
Received: from [60.abc.xyz.215] by web53295.mail.re2.yahoo.com via HTTP; Fri, 09 Jun 2008 14:41:18 -0800 (PST)
Date: Fri, 09 Jun 2008 14:41:18 -0800 (PST)
From: Anne E... <dn...etto@yahoo.com>
Subject: Apple's new iPhone 3G: Live Updates
To: [REDACTED]
Reply-to: dn...etto@yahoo.com
Message-id: <1184649.93759.qm@web53295.mail.re2.yahoo.com>
MIME-version: 1.0
X-Mailer: YahooMailWebService/0.7.289.1
Content-type: multipart/mixed;
boundary=«Boundary_(ID_Hsdus94jJD8d_MukCRm7rsg)»
```

**Intrusion attempt 2 (on March 3rd, 2009)** [48]

- This is a targeted malicious email (TME) attack. The email claimed to be from a legit individual, and was directed to only 5 users that had received similar TME before.

- Malicious attachment in PDF file that could exploit a local unpatched vulnerability in Adobe PDF (CVE-2009-0658) that was announced on 19.02.2009 but not patched until 10.03.2009.

- The weaponized PDF attachment contained 2 files: a benign PDF and an executable backdoor installation file using another 8-bit key encryption algorithm stored in the exploit shellcode. Upon running this file, the shellcode decrypted, placed the backdoor on disk and invoke it while displaying the benign PDF file to the user.

- The backdoor components was extracted. When active, it would send data to the C2 server 202.abc.xyz.7 via valid HTTP requests.

- Email header:

```
Received: (qmail 97721 invoked by uid 60001); 4 Mar 2009 14:35:22 -0000
Message-ID: <552620.97248.qm@web53411.mail.re2.yahoo.com>
Received: from [216.abc.xyz.76] by web53411.mail.re2.yahoo.com via HTTP;
Wed, 04 Mar 2009 06:35:20 PST
X-Mailer: YahooMailWebService/0.7.289.1
Date: Wed, 4 Mar 2009 06:35:20 -0800 (PST)
From: Anne E... <dn...etto@yahoo.com>
Reply-To: dn...etto@yahoo.com
```

53
Table 6.1.2: Intrusion Attempts Indicators (adopted from Hutchins [48])

<table>
<thead>
<tr>
<th></th>
<th>Intrusion 1</th>
<th>Intrusion 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recon.</td>
<td>[Recipient List] Benign HTTP link</td>
<td>[Recipient List] Benign PDF</td>
</tr>
<tr>
<td>Weapon.</td>
<td>Trivial encryption algorithm</td>
<td>Key 1</td>
</tr>
<tr>
<td></td>
<td>Key 2</td>
<td></td>
</tr>
<tr>
<td>Delivery</td>
<td>[Email subject 1] [Email body 1]</td>
<td>[Email subject 2] [Email body 2]</td>
</tr>
<tr>
<td></td>
<td><a href="mailto:dn...etto@yahoo.com">dn...etto@yahoo.com</a></td>
<td>IP: 60.abc.xyz.215</td>
</tr>
<tr>
<td>Exploit.</td>
<td>CVE-2008-5353 [JRE] [shellcode]</td>
<td>CVE-2009-0658 [PDF] [shellcode]</td>
</tr>
<tr>
<td>Install.</td>
<td>C:...\fssm32.exe C:...\IEUpd.exe C:...\IEXPLORE.hlp</td>
<td></td>
</tr>
<tr>
<td>C2</td>
<td>202.abc.xyz.7 [HTTP request]</td>
<td></td>
</tr>
<tr>
<td>Action.</td>
<td>Client machine is compromised</td>
<td></td>
</tr>
</tbody>
</table>

6.2. The checklist and tool support for the decision making method

As introduced in chapter 5, the checklist for security consultants and the tool support have been developed based on the results from our questionnaire that aims to help security consultants and organization to achieve the most appropriate and cost-beneficial investment in security controls. Due to the fact that the checklist and the tool support are both used as the input for the process of decision making method, we evaluate them together with the decision making method itself in the next section.
6.3. The process of decision making method

In this section we present the evaluation of the decision making method process. As mentioned earlier, the evaluation for the checklist for security consultants as well as the tool support would covered here before we go to the main artifact which is our process of decision making method throughout the case study.

6.3.1. Applying the checklist with tool support

At this stage of our case, security consultants had now received information from the organization about the two intrusion attempts happened in 2008 and 2009. We assumed that there could be other attacks happened after 2009 or even before 2008, but based on the historical data from organization, our security consultants could only find evidences for the two intrusion attempts mentioned in section 6.1.

Before we could begin with our process of decision making method, there were some works to do. Firstly, in order to understand the security culture and security baseline of the organization, security consultants needed to talk to different key persons to collect the most relevant and valuable information. These people were typically the Management, risk managers, control owners, ICT manager and some employees’ representatives. The results would then be used as background for conducting risk assessment with help of the checklist and tool support. There are many methods out there in the market to do risk assessment such as Gap analysis, Bowtie, Root cause or CORAS as mentioned in section 4.2. We assumed that whatever method security consultants used in this stage would not have much effect on our results.

At this stage, security consultants could follow all the steps described in section 5.3.

(1) General Information

<table>
<thead>
<tr>
<th>Assessment Name</th>
<th>Spear Phishing Attack</th>
<th>Planned start date</th>
<th>June 1, 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment Owner</td>
<td>Kevin Petterson</td>
<td>Planned end date</td>
<td>July 1, 2017</td>
</tr>
<tr>
<td>Assessment Manager</td>
<td>Mathias Kristiansen</td>
<td>Actual start date</td>
<td>June 15, 2017</td>
</tr>
<tr>
<td>Assessment Status</td>
<td>Done</td>
<td>Actual end date</td>
<td>August 1, 2017</td>
</tr>
<tr>
<td>Other stakeholders</td>
<td>Management, ICT Group, partners, customers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Target / Scope</td>
<td>Security Investment in Security Controls towards Spear Phishing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>The organization has faced two targeted attacks via email attachments known as Spear Phishing Attack. Organization wants to improve security baseline by implementing security controls in order to mitigate risks.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 6.3.1.1: General Information (Result from Tool support)
According to the checklist, this step belonged to *Identifying - Identify organization’s need* group. Organization filled out information in this spreadsheet together with security consultants. The most important thing here was to define the stakeholders and the target of the risk assessment. The results were illustrated as in table 6.3.1.1.

(2) Metadata

Based on our checklist, this step referred back to *Identifying - Identify security controls group*. As mentioned earlier, security consultants didn’t need to do anything here at this stage. However, they had to keep in mind that our metadata could be changed at anytime, so it would be a good idea to keep in touch with all changes made in the industry. For the sake of our case study, security consultants could use these following standards and guidelines:

<table>
<thead>
<tr>
<th>Area</th>
<th>Section</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>A.4.1.1</td>
<td>Criteria</td>
</tr>
<tr>
<td></td>
<td>A.4.1.2</td>
<td>Consistency</td>
</tr>
<tr>
<td></td>
<td>A.4.1.3</td>
<td>Identify risks and owners</td>
</tr>
<tr>
<td></td>
<td>A.4.1.4</td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td>A.4.1.5</td>
<td>Evaluate &amp; mitigate</td>
</tr>
<tr>
<td></td>
<td>A.4.1.6</td>
<td>Documentation</td>
</tr>
<tr>
<td>5</td>
<td>A.5.1.1</td>
<td>Policies for information security</td>
</tr>
<tr>
<td></td>
<td>A.5.1.2</td>
<td>Review of the Policies for Information Security</td>
</tr>
<tr>
<td>6</td>
<td>A.6.1.1</td>
<td>Information security roles and responsibilities</td>
</tr>
<tr>
<td></td>
<td>A.6.1.2</td>
<td>Segregation of duties</td>
</tr>
<tr>
<td></td>
<td>A.6.1.3</td>
<td>Contact with authorities</td>
</tr>
<tr>
<td></td>
<td>A.6.1.4</td>
<td>Contact with special interest groups</td>
</tr>
<tr>
<td></td>
<td>A.6.1.5</td>
<td>Information security in project management</td>
</tr>
<tr>
<td></td>
<td>A.6.2.1</td>
<td>Mobile device policy</td>
</tr>
<tr>
<td></td>
<td>A.6.2.2</td>
<td>Teleworking</td>
</tr>
<tr>
<td>7</td>
<td>A.7.1.1</td>
<td>Screening</td>
</tr>
<tr>
<td></td>
<td>A.7.1.2</td>
<td>Terms and conditions of employment</td>
</tr>
<tr>
<td></td>
<td>A.7.2.1</td>
<td>Management responsibilities</td>
</tr>
<tr>
<td></td>
<td>A.7.2.2</td>
<td>Information security awareness, education and training</td>
</tr>
<tr>
<td></td>
<td>A.7.2.3</td>
<td>Disciplinary process</td>
</tr>
<tr>
<td></td>
<td>A.7.3.1</td>
<td>Termination or change of employment responsibilities</td>
</tr>
<tr>
<td>8</td>
<td>A.8.1.1</td>
<td>Inventory of assets</td>
</tr>
<tr>
<td></td>
<td>A.8.1.2</td>
<td>Ownership of assets</td>
</tr>
<tr>
<td></td>
<td>A.8.1.3</td>
<td>Acceptable use of assets</td>
</tr>
<tr>
<td></td>
<td>A.8.1.4</td>
<td>Return of assets</td>
</tr>
<tr>
<td></td>
<td>A.8.2.1</td>
<td>Classification guidelines</td>
</tr>
<tr>
<td></td>
<td>A.8.2.2</td>
<td>Labelling of information</td>
</tr>
<tr>
<td></td>
<td>A.8.2.3</td>
<td>Handling of assets</td>
</tr>
<tr>
<td></td>
<td>A.8.3.1</td>
<td>Management of removable media</td>
</tr>
<tr>
<td></td>
<td>A.8.3.2</td>
<td>Disposal of media</td>
</tr>
<tr>
<td></td>
<td>A.8.3.3</td>
<td>Physical media transfer</td>
</tr>
</tbody>
</table>

Table 6.3.1.2a: The first areas from ISO 27001:2013 (Result from Tool support)
## SANS Incident Scenarios

<table>
<thead>
<tr>
<th>Incident Scenarios</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IS1</strong></td>
</tr>
<tr>
<td><strong>IS2</strong></td>
</tr>
<tr>
<td><strong>IS3</strong></td>
</tr>
<tr>
<td><strong>IS4</strong></td>
</tr>
<tr>
<td><strong>IS5</strong></td>
</tr>
<tr>
<td><strong>IS6</strong></td>
</tr>
<tr>
<td><strong>IS7</strong></td>
</tr>
<tr>
<td><strong>IS8</strong></td>
</tr>
<tr>
<td><strong>IS9</strong></td>
</tr>
<tr>
<td><strong>IS10</strong></td>
</tr>
<tr>
<td><strong>IS11</strong></td>
</tr>
<tr>
<td><strong>IS12</strong></td>
</tr>
<tr>
<td><strong>IS13</strong></td>
</tr>
</tbody>
</table>

Table 6.3.1.2b: The first 13 Incident Scenarios from SANS (Result from Tool support)

## Lockheed Martin Cyber Kill Chain (CKC)

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CKC1</strong></td>
<td>Reconnaissance</td>
</tr>
<tr>
<td><strong>CKC2</strong></td>
<td>Weaponization</td>
</tr>
<tr>
<td><strong>CKC3</strong></td>
<td>Delivery</td>
</tr>
<tr>
<td><strong>CKC4</strong></td>
<td>Exploitation</td>
</tr>
<tr>
<td><strong>CKC5</strong></td>
<td>Installation</td>
</tr>
<tr>
<td><strong>CKC6</strong></td>
<td>Command and Control (C2)</td>
</tr>
<tr>
<td><strong>CKC7</strong></td>
<td>Actions on Objectives</td>
</tr>
</tbody>
</table>

Table 6.3.1.2c: Lockheed Martin Cyber Kill Chain (Result from Tool support)
## Evaluation of artifacts

### NIST Cybersecurity Framework (CSF)

<table>
<thead>
<tr>
<th>Function</th>
<th>Category ID</th>
<th>Category</th>
<th>Category Description</th>
<th>Subcategory ID</th>
<th>Subcategory</th>
<th>Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID.AM</td>
<td>The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy</td>
<td>ID.AM-1</td>
<td>Physical devices and systems within the organization are inventoried</td>
<td>A.B.1.1, A.B.1.2</td>
<td>CSC 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.AM-2</td>
<td>Software platforms and applications within the organization are inventoried</td>
<td>A.B.1.1, A.B.1.2</td>
<td>CSC 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.AM-3</td>
<td>Organizational communication and data flows are mapped</td>
<td>A.C.2.1</td>
<td>CSC 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.AM-4</td>
<td>External information systems are cataloged</td>
<td>A.C.2.2</td>
<td>CSC 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.AM-5</td>
<td>Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value</td>
<td>A.D.2.1</td>
<td>CSC 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.AM-6</td>
<td>Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established</td>
<td>A.E.1.1</td>
<td>CSC 1</td>
<td></td>
</tr>
</tbody>
</table>

### Identify

| ID.BE    | The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity risk, responsibilities, and risk management decisions. | ID.BE-1 | The organization's role in the supply chain is identified and communicated | A.B.1.3, A.B.2.1, A.B.2.2 |
|          |                                                      | ID.BE-2 | The organization's place in critical infrastructures and its industry sector is identified and communicated | A.B.2.1, A.B.2.2, A.B.2.3 |
|          |                                                      | ID.BE-3 | Priorities for organizational mission, objectives, and activities are established and communicated | A.B.2.1, A.B.2.1, A.B.2.1 |
|          |                                                      | ID.BE-4 | Interdependencies and critical functions for delivery of critical services are established | A.B.2.1, A.B.2.1, A.B.2.1 |
|          |                                                      | ID.BE-5 | Resilience requirements to support delivery of critical services are established | A.B.2.1, A.B.2.1, A.B.2.1 |

### Governance

| ID.GV    | The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environment, and operational requirements are understood and inform the management of cybersecurity risk. | ID.GV-1 | Organizational information security policy is established | A.C.1.1 |
|          |                                                      | ID.GV-2 | Information security roles & responsibilities are coordinated and aligned with internal roles and external partners | A.C.1.1, A.C.2.1, A.C.2.2 |
|          |                                                      | ID.GV-3 | Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed | A.C.1.1, A.C.2.1 |
|          |                                                      | ID.GV-4 | Governance and risk management processes address cybersecurity risk | A.C.1.1, A.C.2.1 |

### Risk Assessment

| ID.RA    | The organization understands the cybersecurity risk to organizational operations (including mission, functions, data, or resources), organizational assets, and individuals. | ID.RA-1 | Asset vulnerabilities are identified and documented | A.D.2.1, A.D.3.2, A.D.3.3 |
|          |                                                      | ID.RA-2 | Threat and vulnerability information is received from information sharing forums and exchanges | A.D.1.4 |
|          |                                                      | ID.RA-3 | Threats, both internal and external, are identified and documented | A.D.1.4 |
|          |                                                      | ID.RA-4 | Potential business impacts and likelihoods are identified | A.D.1.4 |
|          |                                                      | ID.RA-5 | Threats, vulnerabilities, likelihoods, and impacts are used to determine risk | A.D.1.4 |
|          |                                                      | ID.RA-6 | Risk responses are identified and prioritized | A.D.1.4 |

### Table 6.3.1.2d: NIST Cybersecurity Framework (Result from Tool support)

<table>
<thead>
<tr>
<th>Control Area</th>
<th>Family</th>
<th>Area Description</th>
<th>Control</th>
<th>Control Description</th>
<th>Mapping</th>
<th>CSF</th>
<th>CKC</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSC B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malware Defense System</td>
<td></td>
<td></td>
<td></td>
<td>CISC 8.1</td>
<td>Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprises-anti-malware administration tools and event log servers.</td>
<td>Recover (3) Delivery</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CISC 8.2</td>
<td>Employ anti-malware software that offers a centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying an update, automated systems should verify that each system has received its signature update.</td>
<td>Recover (3) Delivery</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CISC 8.3</td>
<td>Limit use of external devices to those with an approved, documented business need. Monitor for use and attempted use of external devices. Configure laptops, workstations, and servers so that they will not auto-run content from removable media, like USB tokens (i.e., “thumb drives”), USB hard drives, CD/DVDs, Firewalls devices, external serial advanced technology attachment devices, and mounted network shares. Configure systems so that they automatically conduct an anti-malware scan of removable media when inserted.</td>
<td>Recover (3) Delivery</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CISC 8.4</td>
<td>Enable anti-intrusion features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc. For increased protection, deploy capabilities such as Enhanced Mitigation Experience Toolkit (EMET) that can be configured to apply these protections to a broader set of applications and executable. Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.</td>
<td>Recover (3) Delivery</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CISC 8.5</td>
<td>Enable domain name system (DNS) query logging to detect hostnames lookup for known malicious C2 domains.</td>
<td>Recover (6) Command and Control (C2)</td>
<td></td>
</tr>
</tbody>
</table>

### Table 6.3.1.2e: Control Area 8 from CIS CSC Top 20 (Result from Tool support)

58
(3-i) Asset Register

Again, this stage of the process related to Identifying - Identify organization’s need group from the checklist. Better than anyone else, organization understood what were important for their business and the whole organization. Based on the two attacks they faced back in time, organization, together with security consultants, defined the assets they wanted to protect, assets that would be harmed if the same attack happened again.

Organization had defined four assets: (A1) Investment Strategy Plan, (A2) Employees’ personal identifiable information, (A3) Partners and customers information, and (A4) Online Banking System. For each asset, organization further defined the CIA (Confidentiality - Integrity - Availability) requirements, whether sensitive information contained or not, the owner, and last but not least the actual value of the asset as well as the cost of consequence in case the asset was harmed. For our case study, we had assumed the value for the CIA requirements, the Value and the Cost of consequence for each asset as illustrated by table 6.3.1.3a.

<table>
<thead>
<tr>
<th>Asset Register</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>A1 Investment Strategy Plan</td>
</tr>
<tr>
<td>A2 Employees’ personal identifiable information</td>
</tr>
<tr>
<td>A3 Partners and customers information</td>
</tr>
<tr>
<td>A4 Online Banking System</td>
</tr>
<tr>
<td>A5 A6 A7 A8 A9 A10</td>
</tr>
</tbody>
</table>

Table 6.3.1.3a: Asset Register (Result from Tool support)

<table>
<thead>
<tr>
<th>Classification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No personal data stored or processed</td>
</tr>
<tr>
<td>Yes - Non-sensitive</td>
<td>Information that can belong to a specific individual, but not sensitive</td>
</tr>
<tr>
<td>Yes - Sensitive</td>
<td>Sensitive information connected to a specific individual (identifiable information)</td>
</tr>
</tbody>
</table>

Table 6.3.1.3b: Classification of Personal Information

Furthermore, organization had also specified consequence scale for each defined asset as following:
### Table 6.3.1.3c: Consequence scale for A1

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>More than 4 Investment Plans affected</td>
<td>(4+) : incident</td>
</tr>
<tr>
<td>Major</td>
<td>3 to 4 Investment Plans affected</td>
<td>(3 → 4) : incident</td>
</tr>
<tr>
<td>Moderate</td>
<td>1 to 2 Investment Plans affected</td>
<td>(1 → 2) : incident</td>
</tr>
<tr>
<td>Insignificant</td>
<td>No Investment Plans affected</td>
<td>(0) : incident</td>
</tr>
</tbody>
</table>

### Table 6.3.1.3d: Consequence scale for A2

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>More than 30 employees affected</td>
<td>(30+) : incident</td>
</tr>
<tr>
<td>Major</td>
<td>11 to 30 employees affected</td>
<td>(11 → 30) : incident</td>
</tr>
<tr>
<td>Moderate</td>
<td>6 to 10 employees affected</td>
<td>(6 → 10) : incident</td>
</tr>
<tr>
<td>Minor</td>
<td>1 to 5 employees affected</td>
<td>(1 → 5) : incident</td>
</tr>
<tr>
<td>Insignificant</td>
<td>No employee affected</td>
<td>(0) : incident</td>
</tr>
</tbody>
</table>

### Table 6.3.1.3e: Consequence scale for A3

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>More than 100 customers affected</td>
<td>(100+) : incident</td>
</tr>
<tr>
<td>Major</td>
<td>31 to 100 customers affected</td>
<td>(31 → 100) : incident</td>
</tr>
<tr>
<td>Moderate</td>
<td>11 to 30 customers affected</td>
<td>(11 → 30) : incident</td>
</tr>
<tr>
<td>Minor</td>
<td>1 to 10 customers affected</td>
<td>(1 → 10) : incident</td>
</tr>
<tr>
<td>Insignificant</td>
<td>No customers affected</td>
<td>(0) : incident</td>
</tr>
</tbody>
</table>

### Table 6.3.1.3f: Consequence scale for A4

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>Affected more than 1 week</td>
<td>(1m+) : incident</td>
</tr>
<tr>
<td>Major</td>
<td>Affected within 1 week</td>
<td>(1m) : incident</td>
</tr>
<tr>
<td>Moderate</td>
<td>Affected within 1 day</td>
<td>(1w) : incident</td>
</tr>
<tr>
<td>Minor</td>
<td>Affected within 1 hour</td>
<td>(1h) : incident</td>
</tr>
<tr>
<td>Insignificant</td>
<td>Not affected</td>
<td>(0) : incident</td>
</tr>
</tbody>
</table>
(3-ii) Threat Agent Register

Security consultants took full advantage of the Threat Agent Library list developed by INTEL to define who Threat Agents were, or could be, as well as their intension, skill and behavior if possible. This step also referred back to Identifying - Identify organization’s need group from our checklist.

Based on Threat Agents’ behavior, evidences from intrusion attempts, and discussion with domain experts, security consultants had addressed two types of Threat Agents:

- **Untrained employee**: non-hostile, internal access, extra-legal (minor) limit, individual resource, none skill, none objective, overt visibility.
- **Mobster**: hostile, external access, extra-legal (major) limit, organizational resource, adept skill, «take» objective, convert visibility.

<table>
<thead>
<tr>
<th>Threat Agent</th>
<th>Type</th>
<th>Access</th>
<th>Motive</th>
<th>Organization</th>
<th>Skill</th>
<th>Objectives</th>
<th>Likelihood</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Untrained employee</td>
<td>Internal</td>
<td>External</td>
<td>Non-hostile</td>
<td>Internal access</td>
<td>Extra-legal (minor) limit</td>
<td>Individual resource</td>
<td>None skill</td>
<td>None objective</td>
</tr>
<tr>
<td>Mobster</td>
<td>External</td>
<td>Internal</td>
<td>Hostile</td>
<td>External access</td>
<td>Extra-legal (major) limit</td>
<td>Organizational resource</td>
<td>Adept skill</td>
<td>«Take» objective</td>
</tr>
</tbody>
</table>

(3-iii) Vulnerability Register

At this stage, security consultants, together with security analysts if required, performed a full vulnerability scan of organization's systems in order to find technical vulnerabilities. Besides, security consultants also implemented compliance check for all processes and internal policies. This step belonged to Identifying - Identify risk group from our checklist. Moreover, likelihood and severity for each vulnerability were defined as well. Table 6.3.1.3h illustrated the results where we assumed the likelihood and severity value for each vulnerably.
## Evaluation of artifacts

### Table 6.3.1.3h: Vulnerability Register (Result from Tool support)

<table>
<thead>
<tr>
<th>Risk Scenario</th>
<th>Likelihood</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1 Do not have network-based tools to detect malware on the network</td>
<td>5 - Almost certain</td>
<td>4 - High</td>
</tr>
<tr>
<td>V2 Unsupported softwares are not updated or removed (e.g., Java, Adobe Flash, Microsoft Office)</td>
<td>4 - Likely</td>
<td>4 - High</td>
</tr>
<tr>
<td>V3 Anti-exploitation features are not implemented</td>
<td>5 - Almost certain</td>
<td>3 - Medium</td>
</tr>
<tr>
<td>V4 Vulnerable systems are not cured</td>
<td>4 - Likely</td>
<td>5 - Critical</td>
</tr>
<tr>
<td>V5 Database with sensitive data is not encrypted</td>
<td>4 - Likely</td>
<td>4 - High</td>
</tr>
<tr>
<td>V6 Do not have Mail Gateway</td>
<td>4 - Likely</td>
<td>2 - Low</td>
</tr>
<tr>
<td>V7 Do not perform scan to find unauthorized softwares</td>
<td>4 - Likely</td>
<td>3 - Medium</td>
</tr>
<tr>
<td>V8 Do not block transmission to known IP addresses and websites that collect stolen information</td>
<td>5 - Almost certain</td>
<td>3 - Medium</td>
</tr>
<tr>
<td>V9 Inappropriate awareness training about spear phishing</td>
<td>5 - Almost certain</td>
<td>4 - High</td>
</tr>
<tr>
<td>V10 Missing policy about personal password and devices</td>
<td>4 - Likely</td>
<td>3 - Medium</td>
</tr>
</tbody>
</table>

### Table 6.3.1.3i: Classification of Likelihood

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>(5) Certain</td>
<td>5 times or more per year</td>
<td>(5+) : 1y</td>
</tr>
<tr>
<td>(4) Likely</td>
<td>3 to 4 times per year</td>
<td>(3 → 4) : 1y</td>
</tr>
<tr>
<td>(3) Possible</td>
<td>1 to 2 times per year</td>
<td>(1 → 2) : 1y</td>
</tr>
<tr>
<td>(2) Unlikely</td>
<td>Less than once per 2 years</td>
<td>(0 → 0,5) : 1y</td>
</tr>
<tr>
<td>(1) Rare</td>
<td>Less than once per 5 years</td>
<td>(0 → 0,2) : 1y</td>
</tr>
</tbody>
</table>

### Table 6.3.1.3j: Classification of severity

<table>
<thead>
<tr>
<th>Rating</th>
<th>Description</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Vulnerability with a potential critical impact on asset</td>
<td>Must be subject to immediate remediation</td>
</tr>
<tr>
<td>High</td>
<td>Vulnerability with a potential high impact on asset</td>
<td>Must be subject to remediation within a short timeframe</td>
</tr>
<tr>
<td>Medium</td>
<td>Vulnerability with a potential medium impact on asset</td>
<td>Must be subject to remediation as soon as possible</td>
</tr>
<tr>
<td>Low</td>
<td>Vulnerability with a potential low impact on asset</td>
<td>Must be subject to consideration and remediation within a reasonable timeframe</td>
</tr>
<tr>
<td>Info</td>
<td>Weakness which in itself does not constitute a direct risk towards asset</td>
<td>n/a</td>
</tr>
</tbody>
</table>

---

62
(3-iv) Risk Register

Besides defining assets and their value, organization had also define the risk matrix, or in other words, «Acceptance criteria for risks» as shown in the table 6.3.1.3g which referred back to Identifying - Identify organization’s need group from our checklist.

Table 6.3.1.3k: Acceptance criteria for risks

<table>
<thead>
<tr>
<th>Rating</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unacceptable</td>
<td>Unacceptable risks. Risk controls must be implemented.</td>
</tr>
<tr>
<td>Tolerable</td>
<td>Major risks. Risk controls should be implemented but are dependent on each individual risk.</td>
</tr>
<tr>
<td>Acceptable</td>
<td>Minor risks. No controls required or could be implemented if affordable.</td>
</tr>
</tbody>
</table>

Table 6.3.1.3l: Description of Risk acceptance criteria

<p>| Risk Register |</p>
<table>
<thead>
<tr>
<th>Description</th>
<th>Threat Agent</th>
<th>Asset</th>
<th>Vulnerability</th>
<th>Severity</th>
<th>Consequence</th>
<th>Existing controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1 Organization is examined and a list of special employees is collected</td>
<td>Mooter</td>
<td>A2 Employees’ personal identifiable information</td>
<td>V8 Inappropriate awareness training about spear phishing</td>
<td>4 - High</td>
<td>4 - Major</td>
<td>3 - High</td>
</tr>
<tr>
<td>R2 Applications are scanned for vulnerabilities</td>
<td>Mooter</td>
<td>A4 Online Banking System</td>
<td>V6 Unsupported software are not updated or removed (e.g., Java, Adobe Flash, Microsoft Office)</td>
<td>4 - High</td>
<td>4 - Major</td>
<td>4 - Very high</td>
</tr>
<tr>
<td>R3 Emails are sent with attachment (e.g. PPT) that contains malicious code</td>
<td>Mooter</td>
<td>A3 Partners and customers information</td>
<td>V6 Do not have Mal Gateway</td>
<td>3 - Medium</td>
<td>3 - Moderate</td>
<td>3 - High</td>
</tr>
<tr>
<td>R4 Malicious code is embedded without involvement of user</td>
<td>Mooter</td>
<td>A4 Online Banking System</td>
<td>V8 Do not perform scan to find unauthorized software</td>
<td>3 - Medium</td>
<td>3 - Moderate</td>
<td>4 - Very high</td>
</tr>
<tr>
<td>R5 Trojan is installed in order to open a backdoor to the infected system</td>
<td>Mooter</td>
<td>A4 Online Banking System</td>
<td>V7 Anti-exploitation features are not implemented</td>
<td>3 - Medium</td>
<td>3 - Moderate</td>
<td>4 - Very high</td>
</tr>
<tr>
<td>R6 Data is sent to C2 server via valid HTTP requests</td>
<td>Mooter</td>
<td>A1 Investment Strategy Plan</td>
<td>V6 Do not block transmission to known IP addresses and websites that collect stolen information</td>
<td>3 - Medium</td>
<td>4 - Major</td>
<td>4 - Very high</td>
</tr>
<tr>
<td>R7 Client machine is compromised. Access is used to attack other systems in the network</td>
<td>Mooter</td>
<td>A4 Online Banking System</td>
<td>V9 Missing policy about personal password and devices</td>
<td>3 - Medium</td>
<td>3 - Moderate</td>
<td>4 - Very high</td>
</tr>
<tr>
<td>R8 Employees download and open attachment with malicious code</td>
<td>Employee</td>
<td>A2 Employees’ personal identifiable information</td>
<td>V8 Inappropriate awareness training about spear phishing</td>
<td>4 - High</td>
<td>3 - Moderate</td>
<td>3 - High</td>
</tr>
<tr>
<td>R9 Employees click on a link and are redirected to malicious website</td>
<td>Employee</td>
<td>A2 Employees’ personal identifiable information</td>
<td>V8 Inappropriate awareness training about spear phishing</td>
<td>4 - High</td>
<td>3 - Moderate</td>
<td>3 - High</td>
</tr>
<tr>
<td>R10 Employees set simple and weak password for their computers</td>
<td>Employee</td>
<td>A2 Employees’ personal identifiable information</td>
<td>V9 Missing policy about personal password and devices</td>
<td>3 - Medium</td>
<td>3 - Moderate</td>
<td>3 - High</td>
</tr>
</tbody>
</table>

Table 6.3.1.3m: Risk Register
Chapter 6  Evaluation of artifacts

Based on all registered assets, threat agents and vulnerabilities, security consultants used this spreadsheet to register risks and related severity, consequence and existing controls (if found) as illustrated in table 6.3.1.3m. This step belongs to Identify - Identify risk group from our checklist. The organization might then categorize each risk into their predefined risk matrix. In this case, the organization did not want to implement this so we skipped this step.

(3-v) Remediation Plan

After all risks had been registered, security consultants, based on industry standards and guidelines from «Metadata», selected proper security controls for each risk in order to mitigate it and reduce the damage to the related asset. This step belongs to Identify - Identify security controls group from our checklist. On the one hand, we could see one control could address more than one risk. On the other hand, we could also observe that one risk required more than one control. Security consultants then calculated the cost of implementation for each risk, either based on their own experience or on the price list provided by vendors. In the same way, security consultants estimated the effect of each controls. This step belongs to Estimating - Estimate cost of security controls implementation / Estimate effect and benefit of suggested security controls group from our checklist. For this case, we assumed the estimated cost, expected effect and benefit for each control as shown in table 6.3.1.3n. Moreover, the role of the organization here was to decide responsible people for each risk and start and finish date.

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
<th>Suggested controls</th>
<th>Estimated cost</th>
<th>Expected effect</th>
<th>Responsible</th>
<th>Planned start date</th>
<th>Planned finish date</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>Organization is examined and a list of special employees is collected</td>
<td>C1</td>
<td>$5,000</td>
<td>3 - High</td>
<td>Mathias Kristansen</td>
<td>August 2017</td>
<td>H1 2018</td>
<td>Planned</td>
</tr>
<tr>
<td>T2</td>
<td>Applications are scanned for vulnerabilities</td>
<td>C2</td>
<td>$2,000</td>
<td>2 - Medium</td>
<td>Mathias Kristansen</td>
<td>September 2017</td>
<td>H1 2018</td>
<td>Planned</td>
</tr>
<tr>
<td>T3</td>
<td>Emails are sent with attachment (PDF, PPT) that contains malicious code</td>
<td>C3</td>
<td>$30,000</td>
<td>3 - High</td>
<td>Mathias Kristansen</td>
<td>October 2017</td>
<td>H1 2018</td>
<td>Planned</td>
</tr>
<tr>
<td>T4</td>
<td>Malicious code is executed without involvement of user</td>
<td>C4</td>
<td>$500</td>
<td>3 - High</td>
<td>Mathias Kristansen</td>
<td>September 2017</td>
<td>H1 2018</td>
<td>Planned</td>
</tr>
<tr>
<td>T5</td>
<td>Trojan is installed in order to open a backdoor to the infected system</td>
<td>C5</td>
<td>$20,000</td>
<td>3 - High</td>
<td>Mathias Kristansen</td>
<td>September 2017</td>
<td>H1 2018</td>
<td>Planned</td>
</tr>
<tr>
<td>T6</td>
<td>Data is sent to C2 server via valid HTTP requests</td>
<td>C6</td>
<td>$500</td>
<td>2 - Medium</td>
<td>Mathias Kristansen</td>
<td>October 2017</td>
<td>H1 2018</td>
<td>Planned</td>
</tr>
<tr>
<td>T7</td>
<td>Client machine is compromised: Access is used to attack other systems in the network</td>
<td>C7</td>
<td>$10,000</td>
<td>2 - Medium</td>
<td>Mathias Kristansen</td>
<td>September 2017</td>
<td>H1 2018</td>
<td>Planned</td>
</tr>
<tr>
<td>T8</td>
<td>Employees download and open attachment with malicious code</td>
<td>C1</td>
<td>$5,000</td>
<td>3 - High</td>
<td>Mathias Kristansen</td>
<td>August 2017</td>
<td>H1 2018</td>
<td>Planned</td>
</tr>
<tr>
<td>T9</td>
<td>Employees click on a fake link and is redirected to malicious websites</td>
<td>C1</td>
<td>$5,000</td>
<td>3 - High</td>
<td>Mathias Kristansen</td>
<td>August 2017</td>
<td>H1 2018</td>
<td>Planned</td>
</tr>
<tr>
<td>T10</td>
<td>Employees set simple and weak password for their computers</td>
<td>C1</td>
<td>$5,000</td>
<td>3 - High</td>
<td>Mathias Kristansen</td>
<td>August 2017</td>
<td>H1 2018</td>
<td>Planned</td>
</tr>
</tbody>
</table>

Table 6.3.1.3n: Remediation Plan
(4) Modeling

Security consultants at this stage modeled the results from the decision making method in order to give organization a clearer risk picture, as well as illustrate the correlation between vulnerabilities - controls - costs. We evaluate the models later in section 6.4.

6.4. The approach to cost-effectiveness modeling

The approach to cost-effectiveness modeling was evaluated partially based on the case study presented earlier in this chapter. The reason we said «partially» is because our case study is not representative enough since the case is not from a real life context. Even though security consultants had followed all phases in the process of decision making method throughout the case study, and were able to provide a list of suggested controls together with its cost of implementation, expected effect and benefit, the number of suggested controls was not enough to create expressive graphs. It is important to keep in mind that we do not said the results from the decision making process was not good enough, just that we need more data for the graphs. For that reason, we assume the number of registered vulnerabilities and controls needed are as illustrated in table 6.4a and 6.4b. Then, we mapped suggested controls as well as vulnerabilities towards Cyber Kill Chain (CKC), Cybersecurity Framework (CSF), and Critical Security Controls Top 20 (CSC) as shown in table 6.4c and 6.4d. We have also assumed the cost of implementation for each CFS function and CSC area illustrated by table 6.4.2 and 6.4.3.

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1</td>
<td>Do not have network-based tools to detect malware on the network</td>
</tr>
<tr>
<td>V2</td>
<td>Do not have proxy to stop traffic from known IP addresses for various types of attacks</td>
</tr>
<tr>
<td>V3</td>
<td>Missing proxy to filter traffic and logging of sessions</td>
</tr>
<tr>
<td>V4</td>
<td>Do not run weekly automated vulnerability scan on the network</td>
</tr>
<tr>
<td>V5</td>
<td>Missing comparison of vulnerability scans to see if previously discovered vulnerabilities are handled</td>
</tr>
<tr>
<td>V6</td>
<td>Anti-exploitation features are not implemented</td>
</tr>
<tr>
<td>V7</td>
<td>Vulnerable systems are not cured (Windows XP and 7)</td>
</tr>
<tr>
<td>V8</td>
<td>Do not have whitelisting of applications</td>
</tr>
<tr>
<td>V9</td>
<td>Do not perform scan to find unauthorized softwares</td>
</tr>
<tr>
<td>V10</td>
<td>Unsupported softwares are not updated or removed (Java, Adobe, Microsoft Office)</td>
</tr>
</tbody>
</table>
### Table 6.4a: Register vulnerabilities (Assumed data)

<table>
<thead>
<tr>
<th>Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>V11</td>
</tr>
<tr>
<td>V12</td>
</tr>
<tr>
<td>V13</td>
</tr>
<tr>
<td>V14</td>
</tr>
<tr>
<td>V15</td>
</tr>
<tr>
<td>V16</td>
</tr>
</tbody>
</table>

### Table 6.4b: Suggested controls mapping towards vulnerabilities (Assumed data)

<table>
<thead>
<tr>
<th>Control</th>
<th>Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1 Network-based anti-malware</td>
<td>V1</td>
</tr>
<tr>
<td>C2 Proxy filter</td>
<td>V2, V3</td>
</tr>
<tr>
<td>C3 Vulnerability scan</td>
<td>V4, V5</td>
</tr>
<tr>
<td>C4 Regular penetrations tests</td>
<td>V4</td>
</tr>
<tr>
<td>C5 Automated patch and software update tool</td>
<td>V10</td>
</tr>
<tr>
<td>C6 Anti-exploitation features</td>
<td>V6</td>
</tr>
<tr>
<td>C7 Secure configuration of OS and software</td>
<td>V7</td>
</tr>
<tr>
<td>C8 App whitelisting / list of authorized app</td>
<td>V8, V9</td>
</tr>
<tr>
<td>C9 Test of 3rd app</td>
<td>V9</td>
</tr>
<tr>
<td>C10 Integrity check of authorized software</td>
<td>V11</td>
</tr>
<tr>
<td>C11 Deny traffic to black lists IP addresses</td>
<td>V12</td>
</tr>
<tr>
<td>C12 Block traffic to well-known file transfer</td>
<td>V12</td>
</tr>
<tr>
<td>C13 Properly configured firewall</td>
<td>V1</td>
</tr>
<tr>
<td>C14 NIDS</td>
<td>V1</td>
</tr>
<tr>
<td>C15 NIPS</td>
<td>V1</td>
</tr>
<tr>
<td>C16 DNS</td>
<td>V12, V15</td>
</tr>
<tr>
<td>C17 Encryption of hardware with sensitive data</td>
<td>V13</td>
</tr>
<tr>
<td>C18 Awareness training</td>
<td>V14</td>
</tr>
<tr>
<td>C19 P2P traffic policy</td>
<td>V15</td>
</tr>
<tr>
<td>C20 Password policy</td>
<td>V15</td>
</tr>
<tr>
<td>C21 BYOD policy</td>
<td>V16</td>
</tr>
</tbody>
</table>
### Table 6.4c: Register vulnerabilities mapping towards CSC, CSF and CKC

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Cyber Kill Chain (CKC)</th>
<th>Cybersecurity Framework (CSF)</th>
<th>Critical Security Controls Top 20 (CSC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1</td>
<td>Delivery / C2 / Actions on Objects</td>
<td>Detect / Protect</td>
<td>CSC 6 - 8 - 9 - 12</td>
</tr>
<tr>
<td>V2</td>
<td>Delivery</td>
<td>Detect</td>
<td>CSC 12</td>
</tr>
<tr>
<td>V3</td>
<td>Delivery</td>
<td>Detect</td>
<td>CSC 14</td>
</tr>
<tr>
<td>V4</td>
<td>Exploitation</td>
<td>Identify / Protect</td>
<td>CSC 4 - 20</td>
</tr>
<tr>
<td>V5</td>
<td>Exploitation</td>
<td>Identify</td>
<td>CSC 4</td>
</tr>
<tr>
<td>V6</td>
<td>Exploitation</td>
<td>Protect</td>
<td>CSC 8</td>
</tr>
<tr>
<td>V7</td>
<td>Exploitation</td>
<td>Protect</td>
<td>CSC 2</td>
</tr>
<tr>
<td>V8</td>
<td>Exploitation / Installation</td>
<td>Identify</td>
<td>CSC 2</td>
</tr>
<tr>
<td>V9</td>
<td>Exploitation / Installation</td>
<td>Identify / Protect</td>
<td>CSC 2 - 18</td>
</tr>
<tr>
<td>V10</td>
<td>Exploitation</td>
<td>Identify / Protect</td>
<td>CSC 4 - 18</td>
</tr>
<tr>
<td>V11</td>
<td>Exploitation</td>
<td>Protect</td>
<td>CSC 3</td>
</tr>
<tr>
<td>V12</td>
<td>Delivery / C2 / Actions on Objects</td>
<td>Detect / Protect</td>
<td>CSC 8 - 12 - 13</td>
</tr>
<tr>
<td>V13</td>
<td>C2 / Actions on Objects</td>
<td>Protect</td>
<td>CSC 13</td>
</tr>
<tr>
<td>V14</td>
<td>Exploitation</td>
<td>Protect</td>
<td>CSC 17</td>
</tr>
<tr>
<td>V15</td>
<td>Exploitation / C2 / Actions on Objects</td>
<td>Detect / Protect</td>
<td>CSC 8 - 15 - 16</td>
</tr>
<tr>
<td>V16</td>
<td>C2 / Actions on Objects</td>
<td>Protect</td>
<td>CSC 15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Controls</th>
<th>Cyber Kill Chain (CKC)</th>
<th>Cybersecurity Framework (CSF)</th>
<th>Critical Security Controls Top 20 (CSC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>Delivery</td>
<td>Protect</td>
<td>CSC 8.2,5</td>
</tr>
<tr>
<td>C2</td>
<td>Delivery</td>
<td>Detect</td>
<td>CSC 12.5</td>
</tr>
<tr>
<td>C3</td>
<td>Exploitation</td>
<td>Identify</td>
<td>CSC 4.1,2,3,6,7</td>
</tr>
<tr>
<td>C4</td>
<td>Exploitation</td>
<td>Protect</td>
<td>CSC 20.1,6</td>
</tr>
<tr>
<td>C5</td>
<td>Exploitation</td>
<td>Identify / Protect</td>
<td>CSC 4.5, 18.1</td>
</tr>
</tbody>
</table>
### 6.4.1. Cost-effectiveness model based on Cyber Kill Chain

Figure 6.4.1 showed a simplified version of our Cost-effectiveness model based on CKC. This simplified model showed us the seven steps in the kill chain, together with seven set of suggested controls. As illustrated, there was a many to many (n:n) relation between the controls and the kill chain steps. In other words, we could see that one or many controls could possibly be used to stop one certain step of the kill chain, and one or many steps could possibly be stopped by a single control.

<table>
<thead>
<tr>
<th>Controls</th>
<th>Cyber Kill Chain (CKC)</th>
<th>Cybersecurity Framework (CSF)</th>
<th>Critical Security Controls Top 20 (CSC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>C6</td>
<td>Exploitation</td>
<td>Protect</td>
<td>CSC 8.4</td>
</tr>
<tr>
<td>C7</td>
<td>Exploitation</td>
<td>Protect</td>
<td>CSC 3.1</td>
</tr>
<tr>
<td>C8</td>
<td>Installation Exploitation</td>
<td>Identify</td>
<td>CSC 2.1,2</td>
</tr>
<tr>
<td>C9</td>
<td>Exploitation</td>
<td>Protect</td>
<td>CSC 18.4</td>
</tr>
<tr>
<td>C10</td>
<td>Exploitation</td>
<td>Protect</td>
<td>CSC 3.5</td>
</tr>
<tr>
<td>C11</td>
<td>Delivery</td>
<td>Detect</td>
<td>CSC 12.1</td>
</tr>
<tr>
<td>C12</td>
<td>C2 / Actions on Objects</td>
<td>Protect</td>
<td>CSC 13.8</td>
</tr>
<tr>
<td>C13</td>
<td>Command &amp; Control (C2)</td>
<td>Detect, Protect</td>
<td>CSC 6.5, CSC 9.6</td>
</tr>
<tr>
<td>C14</td>
<td>C2</td>
<td>Detect</td>
<td>CSC 12.3</td>
</tr>
<tr>
<td>C15</td>
<td>C2</td>
<td>Detect</td>
<td>CSC 12.4</td>
</tr>
<tr>
<td>C16</td>
<td>C2</td>
<td>Detect</td>
<td>CSC 8.6</td>
</tr>
<tr>
<td>C17</td>
<td>C2 / Actions on Objects</td>
<td>Protect</td>
<td>CSC 13.2</td>
</tr>
<tr>
<td>C18</td>
<td>Reconnaissance / Weaponization / Exploitation</td>
<td>Protect</td>
<td>CSC 17.1,2,4</td>
</tr>
<tr>
<td>C19</td>
<td>C2 / Actions on Objects</td>
<td>Protect</td>
<td>CSC 15.7</td>
</tr>
<tr>
<td>C20</td>
<td>Exploitation</td>
<td>Protect</td>
<td>CSC 16.11,12</td>
</tr>
<tr>
<td>C21</td>
<td>C2 / Actions on Objects</td>
<td>Protect</td>
<td>CSC 15.9</td>
</tr>
</tbody>
</table>

*Table 6.4d: Suggested controls mapping towards CSC, CSF and CKC*
6.4.2. Cost-effectiveness model based on Cybersecurity Framework

We assumed the rating of vulnerabilities and costs of implantation as following:

<table>
<thead>
<tr>
<th>Vulnerabilities per CSF</th>
<th>Info</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
<th>Critical</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>$ 6,000</td>
</tr>
<tr>
<td>Protect</td>
<td>0</td>
<td>3</td>
<td>7</td>
<td>2</td>
<td>0</td>
<td>$ 12,000</td>
</tr>
<tr>
<td>Detect</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>$ 3,000</td>
</tr>
<tr>
<td>Respond</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>$ 0</td>
</tr>
<tr>
<td>Recover</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>$ 0</td>
</tr>
<tr>
<td>TOTAL</td>
<td>0</td>
<td>4</td>
<td>9</td>
<td>9</td>
<td>0</td>
<td>$ 21,000</td>
</tr>
</tbody>
</table>

Table 6.4.2: Vulnerabilities per CSF and related costs

As explained in section 5.4.2, here was the Cost-effectiveness model based on CSF:

6.4.3. Cost-effectiveness model based on Critical Security Controls Top 20

We assumed the rating of vulnerabilities and costs of implantation as following:
Chapter 6

Evaluation of artifacts

Table 6.4.3: Vulnerabilities per CSC and related costs

<table>
<thead>
<tr>
<th>CSC</th>
<th>Info</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
<th>Critical</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSC 1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>$ 0</td>
</tr>
<tr>
<td>CSC 2</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>$ 2,500</td>
</tr>
<tr>
<td>CSC 3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>$ 1,750</td>
</tr>
<tr>
<td>CSC 4</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>$ 1,500</td>
</tr>
<tr>
<td>CSC 5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>$ 0</td>
</tr>
<tr>
<td>CSC 6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>$ 3,000</td>
</tr>
<tr>
<td>CSC 7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>$ 0</td>
</tr>
<tr>
<td>CSC 8</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>$ 1,350</td>
</tr>
<tr>
<td>CSC 9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>$ 1,550</td>
</tr>
<tr>
<td>CSC 10</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>$ 900</td>
</tr>
<tr>
<td>CSC 11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>$ 0</td>
</tr>
<tr>
<td>CSC 12</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>$ 250</td>
</tr>
<tr>
<td>CSC 13</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>$ 1,050</td>
</tr>
<tr>
<td>CSC 14</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>$ 0</td>
</tr>
<tr>
<td>CSC 15</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>$ 2,250</td>
</tr>
<tr>
<td>CSC 16</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>$ 1,500</td>
</tr>
<tr>
<td>CSC 17</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>$ 2,550</td>
</tr>
<tr>
<td>CSC 18</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>$ 0</td>
</tr>
<tr>
<td>CSC 19</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>$ 0</td>
</tr>
<tr>
<td>CSC 20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>$ 850</td>
</tr>
<tr>
<td>TOTAL</td>
<td>0</td>
<td>7</td>
<td>8</td>
<td>12</td>
<td>0</td>
<td>$ 21,000</td>
</tr>
</tbody>
</table>

As explained in section 5.4.2, here was the Cost-effectiveness model based on CSF:
6.5. The output of the process of decision method

The output of the process of decision method included:

- A list of suggested security controls based on registered risks, together with the cost of implementation, expected effect and expected benefit of each control.

- A cost-effectiveness model based on Cyber Kill Chain (CKC) that demonstrated the life circle of an intrusion attack including seven steps, together with a set of suggested controls that could possibly be used to stop the attacks at a certain step of the kill chain.

- A cost-effectiveness model based on Cybersecurity Framework (CSF) that showed a total risks picture based on registered vulnerabilities, the correlation between suggested controls and its cost of implementation grouped into CSF function.

- A cost-effectiveness model based on Critical Security Controls (CSC) that illustrated a total risks picture based on registered vulnerabilities, the correlation between suggested controls and its cost of implementation grouped into CSC area.

At this stage of the process, security controls worked closely together with organization and used the checklist to help them select the proper security controls in order to mitigate risks and improve the overall security baseline of the whole organization. This step belonged to Selecting - Select security controls group in our checklist.

Since we used a non realistic case study, that is not in a real life context, it had been a great challenge to come up with an actual outcome. However, there were some points organization could take into consideration while selecting security controls:
• The earlier a control could stop an attack, the more effect that control has since the deeper the threat agent could exploit the target, the bigger consequence it leads to.

• It's not all the time wise to invest in a single very high cost control. Sometimes several minor controls could give the same effect but with much lower cost.

• The cost-effectiveness models showed which security area organization was not vulnerable indicated by the total vulnerabilities found in that area.

6.6. Observations during case study

In this section, we present the observations made by security consultants during the conduct of case study.

For security consultants

• At the beginning, security consultants had difficulties to identify the threat agent since the intrusion attacks happened for many years ago and there was not much historical data from the log provided by organization.

• Security consultants found it quite a challenge to talk to people, specially key people in the organization in order to understand the security culture and risk aversion of the organization.

• Security consultants had a hard time to calculate costs as well as estimate the effect and expected benefit since the case study was not from a real life context, while the cost and effect of controls vary a lot depended on the vendors. Therefore there had been a number of assumptions and uncertainties during the case study.

For organization

• Organization was not quite sure when they asked to identify their assets and its value.

• Organization did not want to categorize risks into the risk matrix.

• Organization got a clearer risk picture, gained more understanding about security controls by learning the cost-effectiveness models provided by security consultants.
Chapter 7

Evaluation with respect to success criteria

In chapter 2, we presented the success criteria for our artifacts: (1) The checklist for security consultants, (2) The development of tool support, (3) The process of decision making method, and (4) The process of decision making method. Then in chapter 6, we evaluated our artifacts through the case study. That brings us to this chapter where we discuss to what extent our defined success criteria for each artifact have been fulfilled.

7.1. The checklist for security consultants

SC 1: Comprehensibility of the checklist

The checklist was created based on our questionnaire and feedbacks, both written and verbal, from domain experts who participated. The content of the checklist was presented in chapter 5, section 5.1. The checklist uses common methodologies adopted from the questionnaire that are familiar to domain experts since all participated domain experts were able to answer all the questions. The checklist contains different standards, guidelines and methods for the conduct of the decision making method. The checklist thus meets some of the security consultants’ needs presented in chapter 2, section 2.1. To an extent, we could claim the comprehensibility for the checklist. However, the comprehensibility of the checklist might vary among security consultants who use the checklist most actively depending on their background and experience. The checklist needs to be evaluated more thoroughly by a larger group of domain experts with different backgrounds and experiences.

SC 2: «Sorting/Grouping» of the checklist

The checklist is composed of three main groups: (1) Identifying, (2) Estimating, and (3) Selecting. The name of each group clearly states the purpose of all check points in that group. Each point in the checklist is grouped into different groups based on its purpose and arranged in the order of implementation.
7.2. The tool support for decision making method

SC 3: Accuracy of the tool support

The tool support as well as its design and components was presented in chapter 5, section 5.2. The tool support was built with Microsoft Excel functions that help to partially automate the data register process for security consultants. For instance, in the «Risk Register» spreadsheet, when security consultants type in the ID of vulnerabilities, the description and severity of that specific vulnerability will be filled automatically. The results were documented in chapter 6. Besides, our metadata from the checklist is correct and up-to-date. The imported data contains the latest version of that particular standard or guideline: ISO27001:2013 Edition 2, Cyber Kill Chain version 2017, Cybersecurity Framework version 1.0 2014, Critical Security Controls Top 20 version 6.1 2016. Nevertheless, our security consultants have to keep in mind that the metadata from the tool support should be updated right away when there is any change in the industry that would affect our metadata, or in case there is any standard or guideline that needs to be imported. The tool support meets the needs of security consultants presented in chapter 2 for «industry standards», «available relevant data», and «knowledge of all the different ways to implement controls».

SC 4: Usability of the tool support

The tool is easy to use since it was developed in Microsoft Excel environment that is very familiar and widely used in academia. As shown in chapter 5 and during the evaluation in chapter 6, the tool provides good and modern user interface. The chosen color set helps the users to find information quicker. Each spreadsheet in the tool support is ordered in the same way as our decision making method so that it is a straightforward work for security consultants as well as organization. All together, the tool support satisfies the need of security consultants mentioned in chapter 2, that is «a well vetted, simple worksheet».

SC 5: Efficiency of the tool support

The evaluation results of the case study presented in chapter 6 indicate that the decision making method is feasible within the allocated resources and acceptable effort, while still providing useful outcome, that is the list of suggested security controls together with its expected cost of implementation, effect and benefit. As for success criterion 4, the tool support fulfills the need of security consultants presented in chapter 2, that is «a well vetted, simple worksheet that can be used across industries and controls». Yet,
since the organization and the presented case are partially fictitious, there is need for further evaluation in a real-life industrial setting with limited resources.

### 7.3. The process of decision making method

**SC 6: Comprehensibility of the decision making method**

The decision making method was conducted based on our checklist and tool support. A description of steps and activities to be conducted by the security consultants during the process of decision making method, including the description of the checklist and tool support, are provided in chapter 5 and thoroughly exemplified through a case study presented in chapter 6. The cost-effectiveness models are also presented. Security consultants, who manage the whole process, were able to interpret the process in a correct manner, followed each step of the process, and delivered the results as expected. Still, the degree of comprehensibility might vary among stakeholders depending on their background and experience, and thus needs further evaluation.

**SC 7: Correctness of the decision making method**

This success criterion indicates that the results security consultants come with after conducting the decision making method should be sufficiently correct. As presented in chapter 6, security consultants are able to provide a list of suggested controls based on registered vulnerabilities and with the help of our metadata that contains most up-to-date and trendy standards and guidelines from the industry. Most just the controls, security consultants also provide expected cost of implementation, effect and benefit for each control. Still, correctness of the results is subject to many factors, such as: different costs from different vendors for various controls or even the same type of control, uncertainty when estimating effect, understanding and experience of security consultants about controls. Therefore, further empirical evaluations of correctness of the decision making method are needed.

### 7.4. The approach to cost-effectiveness modeling

**SC 8: Comprehensibility of the cost-effectiveness models**

As presented in chapter 5 and 6 throughout the use study, the first model gives us the overall picture of a cybersecurity event, an attack life circle, while the last two models illustrate how vulnerable the organization is, how much security controls are needed as well as the corresponding estimated cost of implementation. The models reuse the
terminologies from the checklist in order to create the symmetric relation between different artifacts. The models use common methodologies adopted from the standard (ISO 27001:2013) and guidelines (Critical Security Controls Top 20, Cybersecurity Framework) applied for the case study that are familiar to domain experts. As illustrated in figure 5.4.1, the model uses simple syntax and straightforward flow, while the two graphs 5.4.2 and 5.4.3 use the basic «bar & line» type to illustrate the result. The models thus meet the need of the security consultants presented in chapter 2, section 2.1, that is a «visualization tool».

SC 9: Correctness of the cost-effectiveness models

The presentation of the approach to cost-effectiveness modeling was presented in chapter 5 and the models was exemplified throughout the case study. Our first model was developed based on an industry guideline for cybersecurity namely the Cyber Kill Chain, while the other two models illustrate the output of the decision making process. As long as the output data is correct, the last two models would show the correct illustration of the data in form of graphs. It also means that the security consultants are responsible for delivering correct results. However, regarding our first model, it is still difficult to certainly conclude the correctness of the model since the attack chain could be changed at anytime in the future. Further evaluation is needed and there is space for future work.

SC 10: Expressiveness of the cost-effectiveness models

The presentation and instruction for development of cost-effectiveness models were presented in chapter 5. Our models provide necessary information needed where security consultants and organizations get clearer risk picture and overview of suggested controls compared to its estimated cost of implementation as well as expected effect and benefit. Security analysts indicated that the bar graphs are much more expressive than the data table from the tool support even though they contain the same set of data. Moreover, the color code used and the flow of our first model are demonstrative and provide a sufficient apprehension to all stakeholders. Hence, the models to an extent meet the need of both security consultants and decision makers presented in chapter 2, section 2.1, that is a «Good management dashboards with drill-down capabilities». The last three spreadsheets of the tool support preset three graphs that cover: (1) Vulnerabilities and cost per Cybersecurity Framework function, (2) Vulnerabilities and Cost per Critical Security Controls area, and (3) Controls Status. All together it could be an adequate start for a «good management dashboard».
Chapter 8
Threats to validity and reliability

As mentioned in chapter 7, there are weaknesses in our process of decision making method and cost-effectiveness models. That leads us to this chapter where we take a closer look at some matters that might have some impacts on the validity and/or reliability of our research. According to Runeson and Höst [49], «The validity of a study denotes the trustworthiness of the results, and to what extent the results are not biased by the researchers’ subjective point of view», and there are four aspects of validity that should be addressed: (1) Construct validity, (2) Internal validity, (3) External validity, and (4) Reliability.

8.1. Threats to validity

8.1.1. Construct validity

Runeson and Höst [49] argue that construct validity «reflects to what extent the operational measures that are studied really represent what the researcher has in mind and what is investigated according to the research questions». Back to our case, the construct validity for our research is whether: (i) the checklist and tool support contain what they should, and (ii) the models illustrate what organizations look for. Based on the feedbacks from our questionnaire, domain experts mostly chose one or more predefined options, and sometimes «Other» option. Again, our checklist and tool support are developed based on those feedbacks. We have gathered all responses, including new answers from «Other» option in order to conduct the checklist and tool support. This indicates that the checklist and tool support to a large extent reflect what domain experts have in mind. Our models are also able to illustrate the results that security consultants have come up with. However, since the selection of our domain experts is quite limited, it could lead to the threat of construct validity. Further participation of larger scale of domain experts would help to increase the construct validity of your research.
8.1.2. Internal validity

Internal validity is defined as «the validity of inferences about whether observed covariation between A (the presumed treatment) and B (the presumed outcome) reflects a causal relationship from A to B as those variables were manipulated or measured» [50]. The results from our decision making method and our models to an extent are able to illustrate the correlation between: (i) asset - threat agent - vulnerability - risk - existing controls, and (ii) risk - suggested controls - estimated costs - expected effect - expected benefit with the help of tool support, as well as correlation between (iii) total vulnerabilities - total cost of implementation per security area (both CSC Top 20 and CSF) throughout our models. Nevertheless, it might be argued that one specific cost might have an internal correlation with another cost without at security consultants are aware of. This argument could also be applied to risks and controls in the same way. Still, we need further consideration regarding hidden dependancies. I that manner, the internal validity for our research could be more certainly claimed.

8.1.3. External validity

According to Runeson and Höst [49], external validity «is concerned with to what extent it is possible to generalize the findings, and to what extent the findings are of interest to other people outside the investigated case». Our research has been conducted primarily based on subjective estimates and evaluation from domain experts. Our selected group of domain experts does not represent the large number of stakeholders who would possible take use of our method. Moreover, our artifacts were evaluated just based on one case study and the case was not in a realistic industry context. For those reasons, we might not end up with the fact that our proposed decision making method, together with the checklist for security consultants and the tool support, would give the same comprehensibility, accuracy, usability and efficiency when applied to other case studies in a larger and more complex contexts. However, all the standards and guidelines in the checklist and tool support collected from domain experts have been widely used in different contexts in a real life situations. To the best of our knowledge, our proposed decision making method has been evaluated. Still, it requires further evaluation throughout more cases in a larger and eventually more complex contexts in order to properly confirm the external validity for our research.

8.2. Threats to reliability

Runeson and Höst [49] again dispute that reliability «is concerned with to what extent the data and the analysis are dependent on the specific researchers. Hypothetically, if another researcher later on conducted the same study, the result should be the same». Our research
has been conducted primarily based on subjective estimates from domain experts, since we collect empirical data to develop the security checklist and tool support, through the risk assessment, then the assumption of cost of controls, and the estimation of expected effect and total benefit. For that reason, we might not end up with the same results in the case our proposed process of decision making method is implemented by other security consultants for other organizations. There is no absolute answer or one solution that fits all. There are many other factors that could have an impact on the final selection of security controls, such as organizational strategy, organization’s risk aversion, overhead cost, break-even point (BEP) where attackers move to another target, and not least the people factor. To the best of our knowledge, our proposed decision making method has been evaluated. However, further evaluation should be made in order to claim reliability.
Chapter 9
Conclusions and Future work

Until now we have presented our artifacts and evaluated them through the case study regarding defined success criteria. We have also discussed about weaknesses that lead to threats to validity and reliability for our proposed process of decision making method and models. We have faced lots of challenges during the conduct of this research, yet gained much knowledge. In our last chapter, we first summarize what we have learned so far, then recap what we have done and achieved, followed by a discussion about what can be done in order to improve the quality and validity of our research paper.

9.1. Lesson learned

Indeed, there are quite a few things we have learned while working with this research. First of all, we learned how to conduct a research paper, that is to get to know different research methods, various techniques to collect empirical data, several strategies for evaluation, and how to apply them in our research. Secondly, we learned about various standards and guidelines that are widely used in the market regarding security incidents and security controls. With that knowledge, we have developed a process for decision making method including the checklist for security consultants, the tool support and the cost-effectiveness models. We further evaluate our artifacts through a case study where the results are a list of suggested security controls and their models that provide a clearer risk picture together with corresponding cost of implementation, expected effect and benefit. We also learned how to evaluate the threats to validity and reliability for our research.

During the case study, we have also observed that there are many uncertainties we need to handle. It is the uncertainty when estimating cost for security controls. This cost varies a lot since there are many vendors delivering different tools with different effects and therefore different prices. Moreover, different effect also means uncertainty when we estimate the expected effect of a control, and it leads to the uncertainty when estimating the total benefit. According to the response from domain experts through the questionnaire, some organizations don't even calculate the cost and/or benefit of security controls at all. To an extent, we can see
there is no absolute solution. It is not just about the cost and/or the benefit of controls, it is also about the security culture, risk aversion, and not least the people factor for each individual organization that would have an effect to the selection of security controls.

9.2. Conclusions

In our today’s world where many services have been digitalized, we are facing a great issue with our security and privacy. By security we mean Information Security, or Cybersecurity regarding cyber threats and intrusion incidents, and by privacy we mean our sensitive private information. This does not just affect us as individual, but also have a great impact on enterprises when we consider the problem in a larger scale. As mentioned earlier, Anderson [1] argued that Information Security is traditionally implemented as an afterthought, and security solutions as a result are often reactive rather than proactive. Even when organizations begin to realize the important of Information Security, or in other words security controls to prevent and mitigate risks, it has always been a challenge to balance between the cost and the benefit gained from the selection of security controls corresponding to risks and vulnerabilities. there is still a limitation in the market, that is the lack of sufficient decision making method that combines risk analysis, security controls and cost- effectiveness, together with a support tool that works as a guideline for security consultants as well as organizations.

Our proposed thesis is not trying to find an absolute solution for this problem. What we want to contribute is a more sufficient process of decision making method that supports risk assessment, selection of security controls, and cost-benefit analysis. The method should be:

- useful in the sense that the suggestions of security controls based on its cost and benefit are sufficient;
- comprehensible for the involved stakeholders; and
- cost-effective

In order to achieve the overall research objective, we focus on four main artifacts with its set of success criteria: (1) The checklist for security consultants, (2) The tool support for the decision making method, (3) The process of decision making method, and (4) The approach to cost-effectiveness modeling. Considering the success of our research, we have defined a set of success criteria for each artifact that will later be used in the evaluation process. We have also presented and discussed about the selected research method as well as strategy for evaluation, collection of empirical data and how we have applied them for our thesis. In order to gather empirical data, we have developed a questionnaire and sent to a selected group of
domain experts. Domain experts are people with different backgrounds working in the field of Information Security who have lots of experience regarding risk analysis and security controls. Moreover, domain experts are the one who can give us valuable responses and comments that help to develop the decision making method.

We have also evaluated our artifacts throughout a case study with respect to the predefined success criteria for each artifacts. The results from the decision making method then have been illustrated by our cost-effectiveness models. We were able to provide a list of suggested security controls for each registered vulnerability, together with its estimated cost, expected effect and benefit. Our models were able to give a clearer risk picture for the organizations, as well as to illustrate the correlation between total vulnerabilities - total security controls needed - total cost of implementation.

However, due to the fact that (1) the selected group of domain experts is quite small, (2) our case study is not from a real life context, and (3) there are uncertainties in the estimates, our artifacts needs further estimation in order to properly claim validity and reliability.

9.3. Future work

There are a number of possibilities for future work. Future work should address these following:

The checklist for security consultants

The checklist plays quite an important roll in the process of decision making method since it is used as a «remember list» for security consultants. As mentioned earlier, we developed our checklist mostly based on the questionnaire and the responses from a selected groups of domain experts. One of our weaknesses for this research is that the number of selected domain experts is quite small (20 domain experts received the questionnaire, and we got 17 responses) that the empirical data we collected cannot represent most of the stakeholders who might use our checklist. Therefore, there is room for improvement for both questionnaire and the checklist. By this we mean to plan more interviews with a more variety groups of domain experts, or even conduct an improved version of our questionnaire. In that way we are able to improve the content of the checklist with up-to-date information, as well as enhance the comprehensibility of the check list for all stakeholders.

The tool support for the decision making method

The tool support environment we have chosen for this research is Microsoft Excel. It is a great environment to develop our tool support, and widely familiar both in academia and
among organizations. We tried to implement a section called «Metadata» where we collect different industry standards and guidelines for risk assessment and security controls. However, due to the fact that industry standards and guidelines could change at any time, or that there is need to import more standards and guidelines, it would be really hard to maintain that much data in Excel. For that reason, a kind of application that can be use across operative systems or web-based application with its own database would be a proper improvement in this case. It is also important to keep the tool support as simple as possible regarding future improvements so that it could be efficiently used within limited resource. In addition, there would be a need for access controls, role based (RBAC) for instance, since our tool support process sensitive data of organization. The tool support itself could be considered as an asset for that specific organization.

With the same argument as discussed above for the checklist, the tool support was also developed based on the questionnaire and responses from domain experts. As a consequence, there is need for further evaluation in a larger and more complex context in order to claim the accuracy, usability and efficiency of the tool support.

The decision making method

Our proposed process of decision making method was evaluated with one case study. Another weakness of our research is that our case study is not from a real life context. There are also many uncertainties and assumptions due to the fact that we have experienced a lot of problems while trying to collect empirical data for cost of implementation of different types of security controls, as well as how the effect of a specific control is evaluated. Consequently, future work should address the uncertainty involved in our proposed decision making method. Moreover, further evaluation is required to evaluate the practical feasibility and correctness of our proposed decision making method. By this we mean our proposed decision making method should be evaluated with different case studies from a real life context. In that way we hope to reduce the threats to validity and reliability as discussed in chapter 8 for our method.

The cost-effectiveness models

So far we are able to model the results from the process of decision making method by using flow chart and Excel graphs function. However, there is a threat for the correctness of our model since security consultants have to manually summarize the results, that is to group all registered vulnerabilities and suggested controls together with its cost based on the rating of vulnerability, Cybersecurity Framework functions and Critical
Security Controls area before the graphs can be calculated. An improvement for this issue could be an automated process using existing functions in Excel.

Regarding to the feedbacks from domain experts, there is a need for a “good management dashboard which drill-down function”. Excel is a good environment to develop our tool support and graphs, thus it doesn’t provide any kind of interactive dashboard. For that reason, together with the ambition for a better tool support, another development environment should be considered that could provide better solution for database, interactive dashboards as well as access control.

Overall, the cost-effectiveness models need further evaluation through more case studies with the participation of a larger group of domain experts to increase their comprehensibility, correctness and expressiveness.
Bibliography


   URL: http://www.timgroup.ethz.ch/download.php?ukey=1OTBevOHiFk/k66ABkPSKTIb7KnAz44fNSM9wUE6v4R1nStbXBLGMoHJZBi3T2qs. Accessed 16.03.2015.


[37] Policonomics. 


[40] GNU Octave. 
Accessed 15.05.2015.


URL: http://vserver1.cscs.lsa.umich.edu/~spage/ONLINECOURSE/R4Decision.pdf.  
Accessed 15.05.2015.


Appendices

A. Questionnaire

Introduction

This questionnaire is a part of research work of Tuan K. Pham towards his MSc thesis at Department of Informatics, University of Oslo, Norway.

The research focuses on Cost-Benefit Analysis for investment in the Information Security context.

Objective

The objective of our research is to investigate needs and practices in estimation of cost of security risks, benefits of treating them and selection of security controls.

We kindly ask you to answer the following questions based on your professional knowledge and experience. All provided information will be used anonymously and only for the purpose of this research.

We are very appreciative of you sharing your experience.

Thank you!

General questions

Are you IT security consultant?

- Yes
- No

Your organization / Your client’s organization

Sector

..............................................................................................................................................................................
Multiple Choice Questions

To the best of your knowledge, please answer these following 12 questions (on behalf of ONE client of your choice. You do not need to state who your client is).

Select at least one or several answers for each question. If you have any additional comments, please write in the comment box before you submit this form.

1. How do you / your organization identify risks?
   - Perform Gap analysis
   - Perform risk assessment (e.g. Bowtie, Root cause)
   - Perform vulnerability scan for all systems
   - Perform continuous monitoring
   - Perform log analysis to find possible intrusion patterns based on e.g. signature
• Perform compliance check for all processes and internal policies based on e.g. ISO 27001, Key Risk Indicator (KRI)
• Define and prioritize assets and their value
• Identify Threat Agents based on e.g. INTEL Threat Agent Library (TAL)
• Other

2. How do you / your organization identify possible security controls?

• Brainstorming / Workshop
• Historical/empirical data
• Advice from domain experts
• Based on Confidentiality - Integrity - Availability (CIA) principle
• Based on one or different international industry standards (e.g. ISO 27000 family)
• Based on ISACA Control Objectives for Information and Related Technologies (COBIT 5)
• Based on COSO Enterprise Risk Management Framework
• Based on CIS Critical Security Controls (CSC) Top 20
• Based on NIST Cybersecurity Framework (CSF)
• Other

3. How do you / your organization select security controls to mitigate risks?

• Baseline security approach
• Based on cost-benefit analysis
• Based on personal experience or advice from domain expert
• Based on the effect of risk incidents on organization’s assets
• Low hanging fruits (Quick wins) / "Gut feeling"
• Other

4. Who will take the decision of choosing security controls?

• Management
• Chief Information Security Officer (CISO)
• Security analyst
• IT Architect
5. How do you / your organization estimate the cost of security controls implementation?

- Estimate provided by domain experts based on previous similar projects
- Calculate the net bypass rate for suggested security controls (e.g. 100% bypass rate means the security control is not effective at all)
- Calculate the total of actual damage for each incident type (baseline scenario)
- Calculate Risk-based Return On Investment (ROI)
- Calculate Net Present Value (NPV)
- Calculate direct costs (costs for tools, consulting, etc.) and indirect costs (costs for operation, awareness training, etc.)
- Other

6. Other factors that could affect your / your organization's decision on security investment?

- Internal budget
- Internal security/control culture
- Risk attitude
- Organizational strategy
- Other

7. How do you / your organization estimate the effect of implemented security controls?

- Run questionnaire to estimate Key Performance Indicators (KPIs)
- Base on subjective estimate from domain experts based on similar projects
- Test with use case or real experiment
- Compare with industry statistics and/or market data
- Other

8. How do you / your organization estimate the (monetary) benefit of implemented security controls?

- Estimate potential loss per risk and calculate Single Loss Expectancy (SLE)
- Calculate Annual Loss Expectancy (ALE) and compare with final cost of implemented security controls
• Real Option Analysis (ROA)
• Other

9. How often do you / your organization experience uncertainty related to security cost estimation?
• Most of the time
• Very often
• Often
• Occasionally
• Never
• Other

10. How often do you / your organization experience uncertainty while measuring controls effectiveness?
• Most of the time
• Very often
• Often
• Occasionally
• Never
• Other

11. How do you / your organization express uncertainty?
• Incremental scale
• Quantitative - Ordinal scale (e.g. red = very uncertain, yellow = somehow uncertain, green = quite sure)
• Quantitative - Interval scale (e.g. cost of security controls are 500K — 700K NOK)
• Quantitative - Ratio scale (e.g. the cost for control A would be twice as much as control B)
• Confidence interval
• Probability distribution
• Other
12. When you (your organization) are uncertain about your estimate, what will you do to reduce uncertainty?

- Scale down uncertainty gap based on markets statistic
- Partially/Fully clarify uncertainty based on advice from domain experts
- Make different measurements / testings
- Interview with end users
- Run campaign(s) / demo with end users
- Do thought experiments
- Other

13. What do you think is lacking in the market in order to conduct a better Cost-Benefit Analysis for security controls?

……………………………………………………………………………………………………………………………………………………

14. In your opinion, what is missing or could be improved so that it would be less complicated to visualize and/or handle uncertainty?

……………………………………………………………………………………………………………………………………………………

15. Additional comments

……………………………………………………………………………………………………………………………………………………
B. Results from Questionnaire

General questions

1. Are you IT security consultant?

![Figure B.G.1: Are you IT security consultant?](image)

2. Your organization

Sector

- Healthcare
- Finance
- Public sector
- Information Security
- Retail

Location

![Figure B.G.2: Location (for IT Consultants)](image)

Number of employees (approx.)

- 340
3. Your Background and Role

Position

- Security Analyst
- Senior Advisor IT Security
- Senior Compliance Officer
- Risk Manager
- Managing Consultant, Risk Management & Compliance
- CIO

Education

![Education Chart]

Professional experiences (years)

![Professional Experiences Chart]
4. Your client’s organization

Sector

- Energy
- Finance
- Healthcare
- IT
- IT Services Provider
- Operations / Hosting
- Transport
- Staff
- Private sector
- Public sector

Location

Number of employees (approx.)

- 100
- 120
- 150 (x 2)
- 500
- 5,000
5. Background and Role of your client’s representative

Position

- Analyst
- CISO
- Consultant ( x 2 )
- Corporate Risk Manager
- Cyber Security Analyst III
- Head of IT Security
- Project Manager
- Quality Manager
- Security Coordinator
- Vice President

Professional experiences (years)

- 1 year
- 2 years
- 5 years
- 10 years
- More than 10 years
- 11 years
- 13 years
- 15 years ( x 2 )
- 17 years
- 45 years
Multiple Choice Questions

1. How do you / your organization identify risks?
   
   A. Perform Gap analysis
   B. Perform risk assessment (e.g. Bowtie, Root cause)
   C. Perform vulnerability scan for all systems
   D. Perform continuous monitoring
   E. Perform log analysis to find possible intrusion patterns based on e.g. signature
   F. Perform compliance check for all processes and internal policies based on e.g. ISO 27001, Key Risk Indicator (KRI)
   G. Define and prioritize assets and their value
   H. Identify Threat Agents based on e.g. INTEL Threat Agent Library (TAL)
   I. Other

   **Question 1**

   ![Bar chart showing the results of Question 1]

   Figure B.M.1: Question 1 results

   **Other**: Penetration testing and security incidents

2. How do you / your organization identify possible security controls?
   
   A. Brainstorming / Workshop
   B. Historical/empirical data
C. Advice from domain experts
D. Based on Confidentiality - Integrity - Availability (CIA) principle
E. Based on one or different international industry standards (e.g. ISO 27000 family)
F. Based on ISACA Control Objectives for Information and Related Technologies (COBIT 5)
G. Based on COSO Enterprise Risk Management Framework
H. Based on CIS Critical Security Controls (CSC) Top 20
I. Based on NIST Cybersecurity Framework (CSF)
J. Other

**Figure B.M.2: Question 2 results**

<table>
<thead>
<tr>
<th>Option</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>9</td>
</tr>
<tr>
<td>B</td>
<td>7</td>
</tr>
<tr>
<td>C</td>
<td>11</td>
</tr>
<tr>
<td>D</td>
<td>12</td>
</tr>
<tr>
<td>E</td>
<td>15</td>
</tr>
<tr>
<td>F</td>
<td>3</td>
</tr>
<tr>
<td>G</td>
<td>6</td>
</tr>
<tr>
<td>H</td>
<td>13</td>
</tr>
<tr>
<td>I</td>
<td>3</td>
</tr>
<tr>
<td>J</td>
<td>3</td>
</tr>
</tbody>
</table>

**Other:** NIST 800-83, ISF Standard for Good Practice, Open security architecture

3. **How do you / your organization select security controls to mitigate risks?**
   
   A. Baseline security approach
   B. Based on cost-benefit analysis
   C. Based on personal experience or advice from domain expert
   D. Based on the effect of risk incidents on organization’s assets
   E. Low hanging fruits (Quick wins) / “Gut feeling”
   F. Other
4. Who will take the decision of choosing security controls?

A. Management
B. Chief Information Security Officer (CISO)
C. Security analyst
D. IT Architect
E. Other

5. How do you / your organization estimate the cost of security controls implementation?

Other: Head of IT-security, CCO/COO
A. Estimate provided by domain experts based on previous similar projects
B. Calculate the net bypass rate for suggested security controls (e.g. 100% bypass rate means the security control is not effective at all)
C. Calculate the total of actual damage for each incident type (baseline scenario)
D. Calculate Risk-based Return On Investment (ROI)
E. Calculate Net Present Value (NPV)
F. Calculate direct costs (costs for tools, consulting, etc.) and indirect costs (costs for operation, awareness training, etc.)
G. Other

Other: We don’t calculate costs
Do not estimate cost of controls
Vendor quotes for specific control implementation

6. Other factors that could affect your / your organization’s decision on security investment?
   A. Internal budget
   B. Internal security/control culture
   C. Risk attitude
   D. Organizational strategy
   E. Other
7. How do you / your organization estimate the effect of implemented security controls?

A. Run questionnaire to estimate Key Performance Indicators (KPIs)
B. Base on subjective estimate from domain experts based on similar projects
C. Test with use case or real experiment
D. Compare with industry statistics and/or market data
E. Other

Other: Don’t know

Monitoring and maturity score of controls (security baseline)
Audits, reviews certification

8. How do you / your organization estimate the (monetary) benefit of implemented security controls?
A. Estimate potential loss per risk and calculate Single Loss Expectancy (SLE)
B. Calculate Annual Loss Expectancy (ALE) and compare with final cost of implemented security controls
C. Real Option Analysis (ROA)
D. Other

**Figure B.M.8: Question 8 results**

**Other: Don’t know (x 2)**

**Guess**

**We don’t calculate the benefit (x 4)**

**Not much done recently, but would be on reduce risk (both VAL and EL)**

9. How often do you / your organization experience uncertainty related to security cost estimation?

A. Most of the time
B. Very often
C. Often
D. Occasionally
E. Never
F. Other
10. How often do you / your organization experience uncertainty while measuring controls effectiveness?

A. Most of the time
B. Very often
C. Often
D. Occasionally
E. Never
F. Other

11. How do you / your organization express uncertainty?

A. Incremental scale
B. Quantitative - Ordinal scale (e.g. red = very uncertain, yellow = somehow uncertain, green = quite sure)

C. Quantitative - Interval scale (e.g. cost of security controls are 500K - 700K NOK)

D. Quantitative - Ratio scale (e.g. the cost for control A would be twice as much as control B)

E. Confidence interval

F. Probability distribution

G. Other

12. When you (your organization) are uncertain about your estimate, what will you do to reduce uncertainty?

A. Scale down uncertainty gap based on markets statistic

B. Partially/Fully clarify uncertainty based on advice from domain experts

C. Make different measurements / testings

D. Interview with end users

E. Run campaign(s) / demo with end users

F. Do thought experiments
13. What do you think is lacking in the market in order to conduct a better Cost-Benefit Analysis for security controls?

- A better understanding of what security controls consist of and the importance of having security controls
- An easy way to link the cost of a service to the cost of securing it
- Ways to link cost of service to cost of security
- Knowledge of all the different ways to implement controls; things change very quickly
- A well vetted, simple worksheet that can be used across industries and controls
- First: organizations are different. First Challenge is statistics: 1) cost of experienced Security incidents? 2) then what are the savings (benefit) due to prevented incidents because of functional Security Controls?. Next: analyzing and calculating cost-benefit requires effort and Resources (quantitative approach), though interesting - many organizations don’t have capacity or People to do so
- Objective analysis, clearer measurements
- Benchmarking information
• Empirical data

• Better monitoring and control of network traffic

• The tools and knowledge that would help companies quantitatively assess their risk exposure. I think the cost is much easier to calculate than the benefit.

• Easy accessible and categorized cost/benefit analyses

• Readily available relevant data

• Industry standards

• As mentioned earlier, your question is not a practical approach to security. It’s an academic exercise. Security is a necessary evil (in terms of cost) and degrees of mitigation effort are based on estimated risk levels of key assets and risk appetite of management. It’s not more complicated than that. A cost benefit analysis and data has limited return with regard to management decision to spend money on security efforts.

14. In your opinion, what is missing or could be improved so that it would be less complicated to visualize and/or handle uncertainty?

• Visualization tools

• Visualization apps

• Standard way to calculate

• A well vetted, simple worksheet that could be used across industries and controls

• Difficult, but one way could be to define boundaries by using scenario analysis

• Better tools

• Uniform training of people

• Empirical data

• That’s a huge question. Most humans do not understand uncertainty very well. Drop the risk matrix and remove the human desire to reduce risk and uncertainty down to just one number or qualitative statement.
• More control

• Tools for estimating and reducing uncertainty

• Good management dashboards with drill-down capabilities.

• Industry standards

• "One pager" is what C-suite decision making asks for. What is the cost of the effort? Why is it needed and How and when will it be delivered? Too much calculation and method does not necessarily produce more insight. Look at the cost per insight — it’s an important factor as well.

15. Additional comments

• Great questionnaire!

• Typically our biggest hindrance to implementing security controls is cost
C. Terminology

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Term</th>
<th>Description</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>Asset</td>
<td>Anything that has value to the organization, its business operations and their continuity, including Information resources that support the organization’s mission.</td>
<td>ISO Guide 73:2009</td>
</tr>
<tr>
<td>T2</td>
<td>Consequence</td>
<td>The impact of an unwanted incident on an asset in terms of harm or reduced asset value.</td>
<td>CORAS</td>
</tr>
<tr>
<td>T3</td>
<td>Control</td>
<td>A measure that is modifying risk.</td>
<td>ISO Guide 73:2009</td>
</tr>
<tr>
<td>T4</td>
<td>Data Availability</td>
<td>The fact that data is accessible and services are operational.</td>
<td>ENISA</td>
</tr>
<tr>
<td>T5</td>
<td>Data Confidentiality</td>
<td>The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.</td>
<td>ISO Guide 73:2009</td>
</tr>
<tr>
<td>T6</td>
<td>Data Integrity</td>
<td>The property that data has not been altered or destroyed in an unauthorized manner.</td>
<td>ISO Guide 73:2009</td>
</tr>
<tr>
<td>T8</td>
<td>Impact</td>
<td>The result of an unwanted incident.</td>
<td>ISO Guide 73:2009</td>
</tr>
<tr>
<td>T9</td>
<td>Incident</td>
<td>An event that has been assessed as having an actual or potentially adverse effect on the security or performance of a system.</td>
<td>ENISA</td>
</tr>
<tr>
<td>T11</td>
<td>Probability</td>
<td>Extent to which an event is likely to occur.</td>
<td>ENISA</td>
</tr>
<tr>
<td>T13</td>
<td>Risk</td>
<td>The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.</td>
<td>ISO Guide 73:2009</td>
</tr>
<tr>
<td>T14</td>
<td>Risk acceptance</td>
<td>Informed decision to take a particular risk, can occur without risk treatment or during the process of risk treatment.</td>
<td>ISO Guide 73:2009</td>
</tr>
<tr>
<td>T15</td>
<td>Risk aversion</td>
<td>Attitude to turn away from risk.</td>
<td>ISO Guide 73:2009</td>
</tr>
<tr>
<td>T16</td>
<td>Risk criteria</td>
<td>Terms of reference by which the significance or risk is assessed.</td>
<td>ISO Guide 73:2009</td>
</tr>
<tr>
<td>Ref.</td>
<td>Term</td>
<td>Description</td>
<td>Source</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>T17</td>
<td>Risk estimation</td>
<td>Process used to assign values to the probability and consequences of a risk.</td>
<td>ISO Guide 73:2009</td>
</tr>
<tr>
<td>T18</td>
<td>Risk reduction</td>
<td>Way in which a stakeholder views a risk, based on a set of values or concerns.</td>
<td>ISO Guide 73:2009</td>
</tr>
<tr>
<td>T19</td>
<td>Risk retention</td>
<td>Acceptance of the burden of loss, or benefit of gain, from a particular risk.</td>
<td>ISO Guide 73:2009</td>
</tr>
<tr>
<td>T20</td>
<td>Risk tolerance</td>
<td>Amount and type of risk that an organization is willing to pursue or retain.</td>
<td>ISO Guide 73:2009</td>
</tr>
<tr>
<td>T22</td>
<td>Source</td>
<td>Item or activity having a potential for a consequence.</td>
<td>ISO Guide 73:2009</td>
</tr>
<tr>
<td>T23</td>
<td>Scope</td>
<td>Process for the establishment of global parameters for the performance of Risk Management within an organization. Within the definition of scope for Risk Management internal and external factors have to be taken into account.</td>
<td>ENISA</td>
</tr>
<tr>
<td>T24</td>
<td>Stakeholder</td>
<td>Any individual, group or organization that can affect, be affected by, or perceive itself to be affected by a risk.</td>
<td>ISO Guide 73:2009</td>
</tr>
<tr>
<td>T25</td>
<td>Threat</td>
<td>A potential cause of an unwanted incident.</td>
<td>CORAS</td>
</tr>
<tr>
<td>T26</td>
<td>Threat scenario</td>
<td>Chain or series of events that is initiated by a threat and that may lead to an unwanted incident.</td>
<td>CORAS</td>
</tr>
<tr>
<td>T27</td>
<td>Unwanted incident</td>
<td>An event that harms or reduces the value of an asset.</td>
<td>CORAS</td>
</tr>
<tr>
<td>T28</td>
<td>Vulnerability</td>
<td>The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.</td>
<td>ITSEC</td>
</tr>
</tbody>
</table>