LUND UNIVERSITY

LTH

FACULTY OF ENGINEERING

Guarding against cyber-attacks

A three-step framework

Author:
Martin Österberg

Preword

This report was conducted during the autumn of 2018 and first two months of 2019 as part of my master's in science of Mechanical Engineering, at Lund University. It has sometimes been challenging, but the experience has also been very rewarding.

A special thanks to the organizations and their representatives which I was able to interview for this project, Deloitte, Yubico, Ålandsbanken and an anonymous logistics provider. The results would not have been the same without their support.

Finally, I would like to thank Bertil Nilsson, my supervisor at LTH who has helped me with theoretical questions and always been there when I needed guidance and feedback.

Abstract

Title Guarding against cyber-attacks internally – A three-step framework

Author Martin Österberg, Mechanical Engineering, Faculty of Engineering, Lund University

Supervisor Bertil I Nilsson, Senior Lecturer, Department of Industrial Management and Logistics, Faculty of Engineering at Lund University

Problem Definition Nowadays company information and company operations are greatly dependent on the emerging digital form. With the amount of sensitive data and information circulating online, it is natural that cyber criminals constantly target different companies. It is therefore crucial to have a reliable cyber defense strategy and a well-defined work process to follow in the event of an attack.

Purpose Create a three-step framework for managing/monitoring/preparing the staff for attacks on the IT infrastructure of companies that possesses an IT infrastructure that during a potential cyber attack can experience noticeable damage.

Method The research approach of the thesis is an exploratory methodology, which help in understanding and assessing critical issues of problems. The data collected to support the project is gathered through existing literature, surveys and interviews.

Conclusions Organizations, independent of business area and size are all a potential target for cyber criminals, the threat is evident and organizations constantly need to be on their guard. The three-step framework will help combat these problems by estimating risks and minimizing effects of attacks. This includes implementation of risk management, internal training and protecting technologies. It is essential to have a structured incident response mechanism, where recovery processes are exercised and responsibilities of involved parties are clearly defined. Moreover, the work following an attack needs to identify weaknesses in the recovery processes and the organization as a whole, as well as ensure better resilience in the future by conducting comprehensive post incident analysis.

Keywords Risk management, Business continuity management, cyber/data breach, human error, cyber security/response

Acronyms

Business continuity management (BCM): A process with the purpose to minimize the effects of unanticipated events on the firm's ability to meet customer requirement

Incident Response Plan (IRP): Mitigate the technological, operational and financial impact of a breach, by ensuring that cyber threats are detected, contained and eliminated

Internet of Things (IoT): Data, which is controlled and exchanged for various devices, machines and everyday items that have built-in electronics.

Intrusion Detection and Prevention System (IDPS): A system which analyze and monitor unknown signals, detects known intruder types, threats, processes and methods used. The system sound alarm and notifications when needed.

Milieu: How a series of information technology components need to collaborate, including servers, software products and databases

Maximum tolerable period of disruption (MTPD): The maximum length of time that a service or product can be inoperable without jeopardizing the viability of the organization

Recovery time objective (RTO): The time central services or products would need to be continued in the event of a disruption

Risk Management: Coordinated activities to direct and control an organization with regard to risk

Contents

Chapter 1

The first chapter of the thesis will give context to the problem and briefly introduce the concept of risk and cyber threats. Afterwards, the problem will be explained in more detail and scaled into a manageable form. Then, the purpose and objective will be described, and finally the structure and different chapters will be clarified.

Introduction

1.1 Context of the Problem

The problem in today's industrial society arise from the increasing usage of the digital form. A company today has the majority of systems and business processes all linked through different enterprise resource planning systems where data is exchanged daily. This is of course a must in today's business environment, but also puts companies in a vulnerable position. An incident in the summer of 2017 that attracted attention was when a Nordic company was hit by an attack in the form of a ransomware virus, where users' files were locked. By paying $300 worth of bitcoins, one could unlock the computer and regain access to the files. But problems can remain and need to be act on. This was previously an unknown tampering program and the company's updated Windows system and antivirus protection could not ward off the threat.

Internet of Things (IoT) is another example of how to integrate the physical world closer to computer systems. Via IoT, data is controlled and exchanged for various devices, machines and everyday items that have built-in electronics. This usually results in higher efficiency and accuracy, while simultaneously opening up the company's information center. With so much important data and information that circulates online, it's natural that hackers try to exploit this by infiltrating systems to either sabotage or earn a hack by stealing precious information as well as exerting extortion.

In all types of companies and organizations there are risks in different numbers and magnitudes. It can range from something as simple as reducing the risk of burglary through the implementation of a sophisticated security system to strategic decisions for globally present organizations to reduce the risk of piracy around the horn of Africa, which were a major problem for freight forwarding companies during an hectic time, and still is. Certain risks are easier to protect against, for example, by allowing a third party to take over the risk completely or share it through certain arrangements. Risks that already are known to the organization or obvious risks may already have established methods to take care of it. An example of this is fire risk, which is easily handled by installing fire detectors and extinguishers and communicating to employees what to do in the event of a fire. Then there are risks that can create huge business problems. In case of a crisis that contributes to a business interruption and/or a loss of important processes in the value chain can have devastating consequences. Such a

situation can imply lost image for the organization, as well as important customers and suppliers, which ultimately can put the whole organization in an exposed position.
It is therefore extremely important for companies to have a reliable strategy to protect themselves against this type of threat in an effective manner.

1.2 The Concept of Risk

Risk is a term used daily in a variety of different ways, both within business and everyday life. For example, it can be used in describing likelihood, what is the risk of being hit by a car. It is used as a financial instrument, the risk that this share will decrease in value. Another meaning may be descriptive of a danger; there is a risk that it will begin to burn.
As the term is used so freely it can be difficult to understand its true meaning. Generally it means, a probability or threat of damage injury, liability, loss or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action. (Business dictionary)

The international standard organization (ISO) 9001:2015 explains risk as the effect of uncertainty on an expected result. This definition comprises both positive and negative outcomes of the result. However, the idea is for an approach with risk-based reasoning, with the objective to reduce or prevent negative effects.

According to (Manuj and Mentzer, 2008), risk relevant to global supply chain can be categorized into the following 8 types:

- Supply Risk
- Operational Risks
- Demand Risks
- Security Risks
- Macro Risks
- Policy Risks
- Competitive Risks
- Resource Risks

The listed risk above will be explained further in chapter 4. According to (Kaplan & Garrick, 1981), there are three scenarios that always apply when risk is explained, whatever the context is. And that is, constituted by the answers to the following questions:

- The scenario: What can go wrong?

- Likelihood: How likely is it that it will happen?

- Consequence: What are the focused negative consequences?

This triplet of questions with respective answers outline according to Kaplan & Garrick the first-level definition of risk.

1.3 Cyber-threats

Today, every user of the internet is a part of the cyber world. Through the internet, millions of users, companies and organizations are interconnected. People have shifted their everyday activities to the cyber world as it saves time and is more efficient. The wider use of internet services, such as e-commerce, e-booking, e-advertising and e-banking services, increases the need for cyber security. Cyber criminals are creative and constantly create new ways of infiltration and corruption. However, something that is popular and will always remain popular due to the heavy use of Windows among organizations is the usage of armed macros in Microsoft Office document as a delivery method. In a week in September of 2018 this accounted for 45% of all delivery methods (National Cyber Security Centre)
With constantly evolving methods and new types of malware it is hard to know what to look out for. According to MIT technology review there are 6 major threats to really worry about in 2018:

- Huge Data Breaches
- Ransomware in the Cloud
- Cyber Physical Attacks
- The Weaponization of Artificial Intelligence
- Mining Cryptocurrencies
- Hacking Elections

Cyber criminals can, much like a conventional criminal, commit a vast number of different crimes. Listed below are some types of different cyber crimes.

- Hacking
- Cyber Stalking
- Phishing
- Email Spoofing
- Cyber Terrorism
- Piracy
- Theft
- Fraud
- Distributed Denial of Service
- Harassment
- Mail Bomb
- Form Jacking

The listed threats and crimes above will be explained further in chapter 4. While all these crimes convey problems for organizations there are some more prominent in terms of potential damage to organizations. For instance, people exposed to harassment may suffer immensely, however the crime has minor impact on the operating ability of an organization while a hacking incident could have potentially devastating effects. (Jawad Hussain Awan & al., 2017)

1.4 Problem

Cyber crimes are relatively easy to create and distribute. It is easy to change content and thus shape attacks for different types of businesses. Also, unlike physical crime, one can be on the other side of the world while the attack is initiated. Therefore, it is very important for every company to know how to act in the event of an attack, but is there any useful framework that can resist and support enough? In light of this, the problem to be studied is characterized by the following research questions:

- How to protect against cyber attacks, as well as how to estimate risks and mitigate effects related to cyber threats.

- How to act during an attack, to repair/re-operate and contain the threat.

- How to work after an attack, to reassess security protocols and security strategies.

It is hard to find an absolute solution to the problem at hand. However, by addressing the above research questions in detail, the problem should be manageable.

1.5 Purpose and Objective

It is believed that cyber criminals target companies indifferent of size and business area. Based on this, the purpose of the project is to create a framework for managing/ monitoring/preparing the staff for attacks on the IT infrastructure of companies that possesses an IT infrastructure, which during a potential cyber attack, can experience noticeable damage. The framework will be divided into three parts.

The first part will deal with aspects of estimating risks and minimizing effects related to IT-attacks.

The second part will consider how a company should act during an attack, this include strategies and actions to prevent the spread of tampering programs and how to get the situation under control to prevent further problems to the business.

The third part will consider how a company should work after an attack. This include, creating an understanding of what went wrong and drawing of conclusions/lessons learned, as well as assessing adequate strategies and actions to undertake in order to create better resiliency.

1.6 Delimitations of the Problem

The thesis will on companies with established IT infrastructure and with a number of employees ranging from 25-1000. The framework is intended to be applicable for each business unit in large organizations, and for smaller organizations, which may only have one or two units. It therefore assumes that decisions and actions can be taken on site without confirmation from central management, providing that actions and decisions are taken within the organizational frame of what is allowed and not.
These delimiters imply that large ranges of companies are eligible for analysis. Further, the framework will not focus on specific intrusions and attacks, but instead suggest a holistic approach to guard, react and recover from cyber incidents. The problem studied assumes that an attempt to attack/breach an organization is initiated externally and from unknown initiators without intentional help from the organizations' employees, which is believed to be a realistic assumption.

1.7 Disposition

The thesis is divided into 6 different chapters, which are described below:

- Chapter 2 provides a background to the problem area and discusses companies that recently have suffered from cyber attacks.

- Chapter 3 covers the research methodology and data collection methods used.

- Chapter 4 presents relevant literature related to the problem area. The chapter provides insights in concepts including, risk management, BCM. Furthermore, the chapter covers incident plans, protective technologies and human errors and its relations to cyber security.

- Chapter 5 proposes a framework designed to combat cyber attacks/intrusion, which is inspired by chapter 4 and company studies.

- Chapter 6 starts with a conclusion of the framework, and then assesses how the delimitations have influenced the framework. Then, there is an evaluation if the project objective is reached. Finally, the scientific contribution of the thesis is discussed, and areas for future research.

Chapter 2

The second chapter will provide some background to the problem and describe a selection of notable breaches from 2017 and 2018.

Background

2.1 Preamble

The business environment is constantly evolving, and digitalization is a great part of this. Nowadays, all companies rely heavily on different digital solutions in order to conduct their business. Naturally, with the increased digitalization comes a greater risk for interruptions. Apart from internal complications with machinery or the flow of information another risk is always apparent, which is targeted attacks on the IT structure. Cyber security is an active topic and it is becoming more common for organizations around the world to improve their resilience to well-organized cyber attacks. Continents with highly developed IT infrastructure including North America, Europe, East Asia and the Pacific all consider cyber-attacks to be the biggest threat to doing business. The number of violations or attacks increases by 27.4% per annum, and in 2017, 86% of the world's companies reported that they were in some way exposed to a cyber incident. (Lloyd's Register & WEF)

This is exactly what happened to a worldwide operating Nordic company during 2017. This attack, which completely inhibited most processes and their ways to do business, gave birth to this thesis idea. An external estimate of total costs for this cyber attack was $300 million. It became apparent that it is vital to have a clear and structural way to deal with this type of attacks. It is interesting to know how to estimate and mitigate risks related to attacks in order to prevent them in the best possible way, also that there is a predetermined way to work during an incident. And finally, that there is a continuation plan for the work following the attack.

2.2 Notable Breaches 2017/2018

In order to provide further context to the problem, this section will describe a few incidents that are relevant to understand what type of threats organizations potentially are exposed to.

WannaCry – May 2017

The WannaCry ransomware attack took place in May 2017 and infected tens of thousands of systems in 150 different countries and spread quickly across a range of industries. The malware, which targeted outdated Windows software, locked down the computer systems while awaiting payment. The financial loss is estimated at $4 billon. (CNN)

Equifax – July 2017

Equifax, which is one of the largest credit bureaus, operative all around the world was in July 2017 penetrated by cybercriminals. The perpetrators stole data of 145 million people. An attack of this magnitude is catastrophic, especially since the stolen information contained social security numbers, which can be used for identity theft and creation of false identification documents. The financial loss is estimated to $600 million. (CNN Business)

Facebook – March 2018

In March 2018 Facebook had to answer for a scandal concerning a massive personal information leak. A political data firm called Cambridge Analytica gathered personal information from more than 50 million users through an app. The app collected information from users such as personalities, activities on the platform and social networks, which Cambridge Analytica then used for political purposes.
This led to an intense debate regarding Facebook's and other tech companies' use of data. (Alert Logic)

British Airways – September 2018

The summer of 2018 hackers targeted British Airways. The hackers did not disrupt the systems by cracking the company's s encrypted data, which often is the case. Instead they gained unauthorized access to the airline's system. Information used to do bookings and reservations were compromised during a ten-hour window. Hackers obtained information from an estimate of 400 000 payments. Information compromised consisted of addresses, names, credit card numbers, expiry dates and even the three-digit security code. This information, all together, makes it quite simple to make fraudulent transactions. (The Telegraph)

2.3 Cybersecurity Costs and Facts

It is essential to have a general understanding of metrics related to cyber issues, and the potential costs related to cyber crimes. The list presented below provides some examples of costs and facts related to cybersecurity: (Varonis)

Costs:

- Malware attacks on a company normally costs the company $2.4 million.
- The general cost in time of a malware attack is 50 days.
- In 2017 the cost of ransomware damage exceeded $5 billion, 15 times the cost in 2015.
- The most expensive component of a cyber attack is information loss, which represents 43 percent of costs.
- The damage related to cybercrimes is estimated to hit $6 trillion annually by 2021.

Facts:

- Ransomware detections are more dominant in countries with higher numbers of internet-connected populations. United States is ranked the highest with 18.2 percent of all ransomware attacks.
- Microsoft Office formats represent the most prevalent group of malicious file extensions at 38 percent of the total.
- Over 20 percent of cyber attacks in 2017 came from China, 11 percent from the United States and 6 percent from Russia.
- In 2017, spear phishing emails were the most commonly used vector to initiate an attack, estimated at 71 percent.

The examples mentioned above provides a general understanding of what cyber attacks convey in terms of cost, as well as were attacks originate from and what type of infection vectors that are commonly used.

This section together with the scenarios covered on the previous page highlight the importance of the issue and provide context to what the framework ultimately will need to support.

Chapter 3

The third chapter explains the research methodology. Firstly, the research approach is described, followed by the research design. Finally, there is an explanation of how the data has been acquired.

Methodology

3.1 Approach

In order to carry out a scientific project in which the researcher can validate and describe the choices and approaches made, the project is required to follow an elaborate and proven method that supports the project. There are different research methods used to conduct a study and the method should be of a scientific nature and be appropriate to the problem in question. The methodology underlying this project is an exploratory research method together with an element from the descriptive research method.

According to (S. Sreejesh, Sanjay Mohapatra, M. R. Anusree, 2014) an exploratory study helps in understanding and assessing critical issues of problems. These types of studies are conducted for three main reasons, to analyze a problem situation, to evaluate alternatives and to discover new ideas. This method fits well with the project objective, which is to create a framework that companies with integrated IT systems can follow in order to manage/monitor attacks on the IT infrastructure.

Since companies are victimized independent of field it is believed that a wide range of companies match the profile including consultancy firms, manufacturing firms, banking firms and service providers. The goal is to interview one or more companies from these branches. It is believed that this will generate interesting and diversified responses to how companies' reason concerning security against IT attacks and IT intrusions. Collected data along with theory covering identification, mitigation, and prevention of external risks and threats will lay the foundation of the framework. Thus, the results and summary will consist of academic literature and collected qualitative data.

In order to receive constructive critique and comments will at least one of the interviewed companies review the framework. The framework will consist of 3 parts, which systematically describe how an attack or intrusion should be prevented, handled in an ongoing situation and addressed in the aftermath of the attack to create better resiliency.

Models and literature considered appropriate for answering the problem will create a structure that will be followed during the development of survey questions and interviews. Information and data provided by companies will then be analyzed in accordance with the theory and models in order to create the framework.

3.2 Research Design

Data will be gathered from survey studies and interviews to support the described problem. This information gathering technique fits the research design, which is based on the main steps from exploratory research proposed by (S. Sreejesh, Sanjay Mohapatra, M. R. Anusree, 2014) with some customization by the author and is structured like the following:

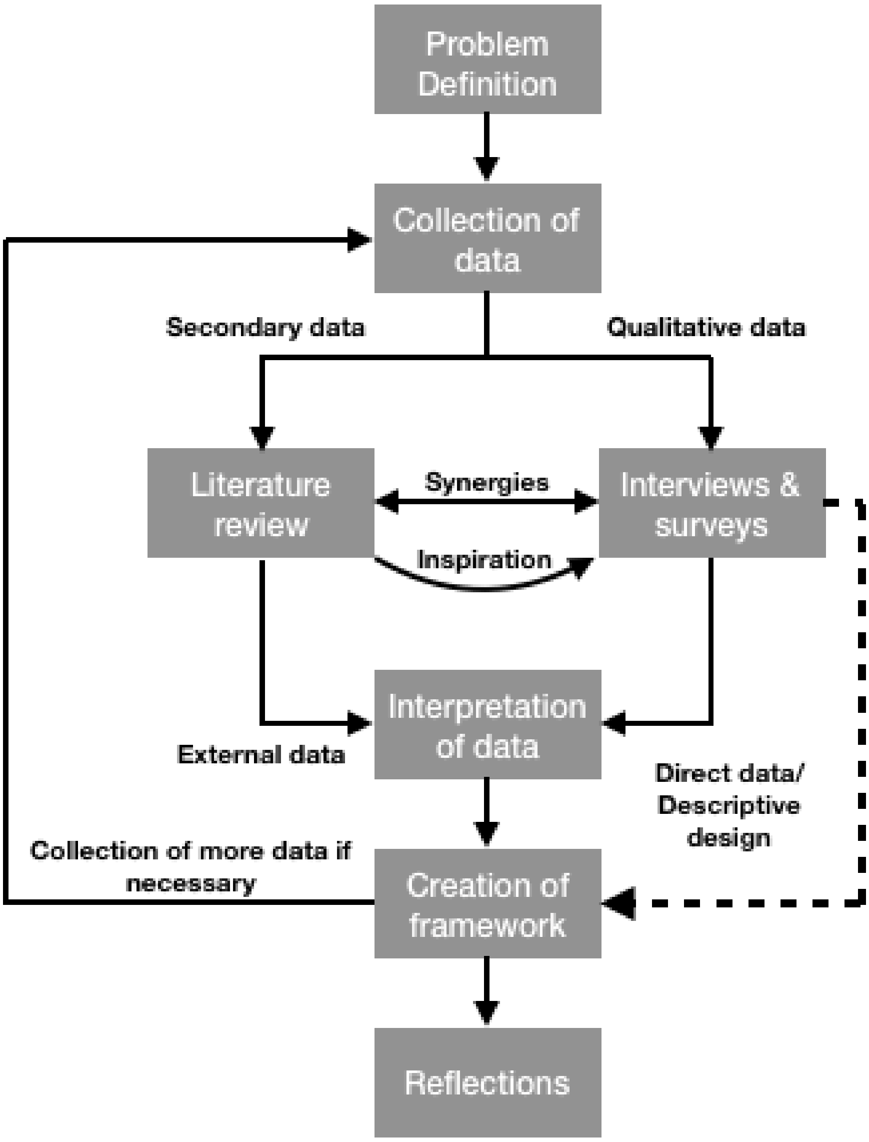


Figure 1. The explorative research design with the descriptive survey element of the thesis (author´s)

The exploratory design collects secondary data and qualitative data. The secondary source of data is then divided into internal and external.

- Internal sources of secondary data are those that can be accessed inside an organization. Examples of this type of data are production summaries, departmental reports, financial and accounting reports, and marketing and sales studies.

- External sources of secondary data are those that are accessible outside a company. This type of data come in forms of books, government sources, computer-retrievable databases, publications, media sources and commercial sources to name a few.

The secondary data in this thesis are constituted exclusively by external data since there is no official collaboration between the author and the involved companies.

The qualitative data in an explorative design is gathered from either direct or indirect sources. The indirect data is collected through projective techniques while the direct data comes from focus groups or direct interviews, which is the case in this thesis.

The second part of the acquired qualitative data comes from surveys, which originates from the descriptive research design where the information is collected by asking a set of pre-formulated questions in a predetermined sequence in a structured questionnaire to a sample of individuals.

3.3 Data Collection Method

3.3.1 Literature Review

From academic literature, theoretical models related to risk management, BCM and IT security will be used. The literature will mostly consist of previous research from business journals, books and scientific papers. The search engine LUB search available from Lund University has primarily been used. This search engine was selected because it was deemed to be the most comprehensive, offering a wide variety of printed information, including electronic journals, books and articles. Keywords used include, risk management, BCM, cyber/data breaches, human error, and cyber security/response. These search words were used since they are quite comprehensive and constitute a solid foundation for the described problem. Articles and journals generated from these words often gave rise to new information and buzzwords, which produced further adequate literature. Additionally, information from the Internet, including pages from governments, news agencies and articles has been used.

3.3.2 Surveys and Interviews

Typical survey objectives involve describing or learning from an ongoing activity by studying the changes in behavioral patterns of the subjects of interest to the researcher (S. Sreejesh, Sanjay Mohapatra, M. R. Anusree, 2014). Based on this, surveys are of descriptive nature and often convey quantitative data. However, surveys also tend to entail qualitative aspects, which is the case of the surveys in this thesis. The surveys discuss questions related to the three different parts, which also include more underlying and detailed questions to each part. The following survey questions are holistic and structured similarly to the research questions presented in chapter 1:

- Part 1, what is the strategy for mitigates risk for cyber attacks, what do the company consider relevant?

- Part 2, how should the alleged company work during an attack? What is the point of action?

- Part 3, what is important to consider in the aftermath of an attack? Does an action plan exist?

The questions present above will also serve as the foundation during interviews, and in the prolongation the entire framework.

The interviews were held over phone with an average discussion of 40 minutes. The goal during the interviews was to develop a rewarding discussion based to these questions in order to understand how companies address these problems and where priorities lie. The interviewed representatives had the prerequisite of either working with cyber security or having a management position. The guides that were used for interviews and surveys can be seen in appendix (A1) and appendix (A2) respectively.

3.3.3 Interpretation of Data

During the literature review phase of the methodology a wide range of previous articles, journals, books, and web pages have been assessed. While a lot of data were related to the area of risk and cyber security, did not everything support the established problem and purpose of the thesis. With this in mind, the author has only selected secondary data that were deemed relevant, which is presented in the following chapter. The selected data served as inspiration to the interviews and surveys, which in turn provided new viewpoints. The results from interviews and surveys have been analyzed both separately and in accordance with theory in order to identify new ideas and similarities, which the framework could be built on.

3.3.4 Limitations of Sources in Data Gathering

The framework will focus on organizations individually, independent of upstream suppliers and downstream customers since it is believed to be hard and too time consuming to gather information from an entire network.

3.4 Creation of Framework

The framework foundation in this thesis is based on relevant concepts drawn from adequate literature, own experience and qualitative data in the form of surveys and interviews. Each part of the framework has been created systematically; where recommendations and guidelines are founded on the previous mentioned literature in accordance with analyzed qualitative data. In addition, original ideas and approaches learned from the interviews and surveys have been implemented directly. Finally, figures and tables introduced in the framework are sometimes adapted from literature, as well as created through interpretation of acquired information.

Chapter 4

The fourth chapter will review key topics from the literature related to risk processes and cyber security. The literature covered in this chapter together with interviews and surveys will serve as the foundation when developing the framework.

Theoretical Framework

According to Manuj and Mentzer, risk relevant to global supply chain can be categorized into the following 8 types:

Type of Risk	**Source**
Supply Risk	Disruption of supply, inventory, schedules, and technology access; price escalation; quality issue; technology uncertainty; product complexity and frequency of material design changes
Operational Risks	Breakdown of operations; inadequate manufacturing or processing capability; high levels of process variations; changes in technology and changes in operating exposure
Demand Risks	New product introductions; variations in demand (fads, seasonality, new product introductions by competitors and chaos in the system (the Bullwhip effect on demand distortion and amplification)
Security Risks	Information systems security; infrastructure security; freight breaches, from terrorism, vandalism, crime and sabotage
Macro Risks	Economic shifts in wage rates, interest rates, exchange rates, and prices
Policy Risks	Actions of national governments like quota restrictions or sanctions
Competitive Risks	Lack of history about competitor activities and moves
Resource risks	Unanticipated resource requirements

Table 1. Risk types and where the originate from, adapted from Manuj and Mentzer (2008)

With constantly evolving methods and new types of malware it is hard to know what to look out for. According to (MIT Technology Review) there are 6 major threats to really worry about in 2018:

- **Huge Data Breaches**
  It is thought that companies holding sensitive information will be targeted, especially those holding information regarding personal web browsing habits.

- **Ransomware in the Cloud**
  This is what happened to the already mentioned Nordic company and this type of method has been used considerably. Ransomware is a quite simple form of malware. The idea behind it is locking down personal computers and files. The intruder then demands a ransom payment.

- **Cyber Physical Attacks**
  This type of attacks targets different critical infrastructure, for instance transportation systems, electrical grids and hospitals. Hackers then normally demand a ransom in order to give up control.

- **The Weaponization of Artificial Intelligence**
  Researchers and security firms have been using artificial intelligence (AI) technologies in order to better anticipate new incoming attacks and to spot attacks that are ongoing. In response to this it is very likely that hackers will strike back by adopting the same technology. Also, it is believed that hackers will use AI in order to design malware with improved ability to fool security systems.

- **Mining Cryptocurrencies**
  Lately, hackers have been targeting holders of Bitcoin and other cryptocurrencies. However, theft of cryptocurrencies is not the biggest problem. It is the processing power needed to mine or crack these currencies. Hackers seek to overtake millions of computers in order to use them for this purpose. Naturally, when suitable targets get compromised, such as hospital chains, airports and other delicate locations, the collateral damage is evident.

- **Hacking Elections**
  Nowadays, in order to reach as many people as possible and get maximum exposure, elections are greatly dependent on media and the presence in the digital world. In turn, this creates opportunities for hackers to influence elections by spreading false and misleading information. Notable is the 2016 presidential election in the United States where hackers targeted voting systems in several states.

The following list provides an explanation of some common crimes, which was mentioned in the introduction chapter.

Type of crime	Objective
Hacking	When a computer system or computer network is exploited
Cyber Stalking	Harassment of a group, an individual or an organization via the internet
Phishing	Phishing is fraud trick which is used for identity or information theft
Email Spoofing	Email spoofing is used to create email messages with a fake sender address
Cyber Terrorism	Activities with the objective to harm, threaten and create large-scale disruption of computer networks
Piracy	Piracy is associated with violation of copyrights
Theft	When property is taken without the consent of the alleged owner
Fraud	Illegal gain via deliberate deception
Denial of Service	Prevent normal activity of systems, normally achieved by routing a vast amount of traffic to a system in order to crash it
Harassment	Different behaviors of threating nature
Mail Bomb	An activity with the objective to hang the functioning server of a specific user or system
Form Jacking	Infect web sites with malicious code designed to steal credit card details and other sensitive purchasing information

Table 2. An explanation of some common cyber crimes (author´s)

The content in the table above should not be seen as exhaustive, since there are a large number of different cyber crimes.

4.1 Asymmetric Threats

Risk management and crisis planning often focus on specific potential issues, but equally important and far more complicated is how to prepare for unforeseen threats that arise out of nowhere. Threats of this nature are referred to as asymmetric threats, which imply some sort of surprise element or blind spot; characterized by the low probability of occurrence versus the massive costs for preparing for this type of event and the enormous costs and destruction if it happens. A major challenge for organizations is to find a strategy to mitigate these unpredictable threats without utilizing too many resources on various assessments, squandering money on overall strategies to cope with a variety of potential crisis or having several departments developing preventative measures individually. (Strategy and Business)

The combination of factors present makes these threats highly irregular. According to a PwC survey on crisis management, 30% of the chief executives expect to be hit by some kind of crisis in the next three years. (PwC)

According to Strategy and Business there are four wide classes of asymmetric threats:

- Unprotected Infrastructure
- Vulnerable Technology
- Underestimated Disasters
- Innovative Geopolitical Attacks

Naturally, it is very important to consider all of these threats when establishing crisis prevention functions. However, the risk assessment models in this chapter will later be used to cope with threats associated with vulnerable technology.

4.2 Risk Management

Risk management is according to ISO defined as 'coordinated activities to direct and control an organization with regard to risk'. Furthermore, risk management is according ISO 31000:2018 constituted by the following 7 steps:

- Communication and Consultation

- Establish Context

- Risk Assessment
  - Risk Identification
  - Risk Analysis
  - Risk Evaluation

- Risk Treatment

- Monitoring and Review

Implementation will support the organization when managing risks and the steps will now be described in more detail.

4.2.1 Communication and Consultation

This step includes communication within parties that are responsible for the implementation of necessary risk management processes. This step is relevant since it is important that everybody involved in the process understand the basis on which decisions are made and why certain actions are required. Also, communication and consultation between involved parties is important since it provides a different point of view, seeing that judgment regarding risk may vary among parties depending on how concerns, values, needs and assumptions are perceived. (Australian Government, p. 10)

4.2.2 Establishing the Context

The second step in risk management is to establish the context. In order to do this, it is important to understand the entity´s or considered process' objective, goal and operating environment. Risks need to be managed in harmony with the goals and objectives of the organization. If they are managed in isolation, any risk management action will provide little or no support to these objectives. Another central component is to identify the objectives that one is trying to achieve. These can be program objectives, project objectives or organizational objectives. The entity's corporate plan is usually a helpful place to start looking. Further, it is important to define external and internal parameters concerning risk management. This include that the entity understands and take into account the objectives of the external stakeholders when developing risk criteria. Further, understanding the entity's internal coherence is equally important since this will affect the way an organization handle risk. (Australian Government, p. 2)

4.2.3 Risk Identification

Risk identification is a process where the organization aims to find, recognize and describe different risks, as well as identifying scenarios, events, actions and other external influences that may give rise to risk. There are several different methods and techniques to identify risks. However, the process is most effective when important stakeholders are present in structured brainstorming workshops, where the output from the previous step should support the discussions. Depending on how well the assessor has understood the objectives and goals of the entity will directly inflict the quality and relevance of identified risks. Apart form brainstorming there are other identification methods, which include such as work breakdown analysis, risk breakdown analysis and expert facilitation. Furthermore, the identification of consequences is equally important. The consequences of a risk are the outcome of the risk being realized. Through understandings of the realistic consequences are essential and permit appropriate categorization of severity. (Australian Government, p. 3-5. & Chadist Patrapa)

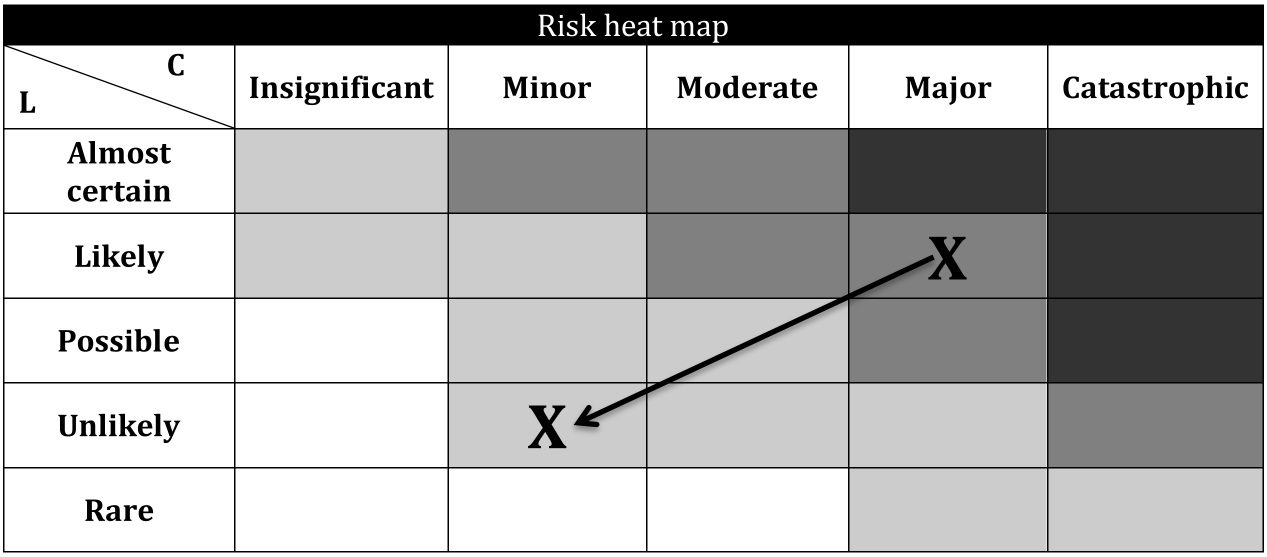
4.2.4 Risk Analysis

Risk analysis is a process with the objective to understand the nature and level of identified risks. In order to establish the inherent risk, the process considers possible sources, causes and their likelihood and consequences, which is specifically important. There is an important difference between risk analysis and risk evaluation. The prime focus of risk analysis is to understand the identified risks as good as possible. Whereas the risk evaluation focus on what risks that are most important to the entity based on their goals and objectives. The analysis can be carried out with different level of detail. Depending on the circumstances, it can also differ in terms of analysis method. In general, either a quantitative or a qualitative analysis is conducted, as well as a combination of both. A quantitative method typically includes allocation of appropriate quantitative measures for likelihood and consequences to the identified risks. (Chadist Patrapa & Australian Government, p. 5-7)

Likelihood
A calculation based upon information and data available from past events is normally drafted in order to understand how probable an event is to be realized. The likelihood is normally represented from not likely/rare to almost certain and the criteria need to be in conformity with the organization and its needs.

Consequence
Consequence is much like likelihood a calculation based upon historical data and experience from past risk events being realized. The established criteria have to reflect significant impacts that are relevant to the organization.

Risk Severity
Risk severity is a calculation based on the likelihood and consequence rating of a risk. Risk severity is usually demonstrated through a two-axis risk matrix, with likelihood on one axis and consequences on the other axis. Once likelihood and consequence have been assigned to a risk, a heat map or risk matrix will give an overall rating of the risk. Naturally, it is vital that the elements in the risk matrix are well calibrated and reflect the organizations tolerance and appetite for risk. Otherwise, there is chance that too much or too little effort is put into risks with incorrect ratings.



Risk heat map

C L	Insignificant	Minor	Moderate	Major	Catastrophic
Almost certain	░	▒	▒	▓	▓
Likely	░	░	▒	▒ X	▓
Possible		░	░	▒	▓
Unlikely		░ X	░	░	▒
Rare				░	░

Figure 2. Risk in relation to likelihood and consequence, adapted from Australian Government

4.2.5 Risk Evaluation

The risk evaluation process determines the tolerability of each risk. Tolerability help to determine which risks and/or its magnitude that are acceptable or if it needs treatment with the relative priority. Further, this is achieved by comparing risk severity from the analysis with the already established risk criteria. For instance, an organization might decide that risks above a certain severity are intolerable while risks below this severity are acceptable. However, an entity cannot function without any risk elements and it is commonly known that sooner or later organizations are exposed to risk. Based on this it is very important that the people in charge within an organization are prudent while deciding what level of risk the organization is comfortable with being exposed to. This is also known as the organizations risk appetite, and it should be communicated within the organizations risk framework. Details of the appetite should concern when the organization can tolerate higher levels of risk, under what circumstances and with what level of control. (Australian Government, p. 7-8)

4.2.6 Risk Treatment

Risk treatment is a process where the appropriate methods to alter or modify the alleged risks are selected and implemented. It is a cyclical process where the treatment methods are assessed to ensure that the residual risk, which is the risk that remains after a treatment has been assigned and implemented, is brought to a tolerable level. Suitable treatment to implement is based on the evaluation in the previous step. Typical options to consider include the following: (Enisa & Australian Government, p. 8)

- Avoid the risk by not starting or terminate the process that gives rise to the risk.

- Sometime the risk can be accepted through well-informed and well-discussed decisions or if it is deemed negligible.

- Share or transfer the risk with other parties that face the same risk for instance by entering insurance arrangement. Organizations can also share the risk by altering the organizational structure, for instance by entering partnerships or joint ventures. By doing this, the responsibility and liability are divided, but a new risk emerge in terms of the new organization might not be able to manage the risk properly.

- Modify the consequences of the risk in such way that losses are reduced.

- Modify the likelihood of the risk, trying to mitigate or eliminate the likelihood of negative outcomes.

The presented risk transfer list is comprehensive, and the options should be applicable on a variety of risks.

4.2.7 Monitor and Review

Monitoring and reviewing is an important step in the risk management process where responsibilities are clearly defined among all involved. All aspects of the process are covered with the following intentions:
(Australian Government, p. 10-11)

- It needs to be assured that controls are efficient and effective in terms of design and operation.
- Gather information to improve the risk evaluation process.

- Analyze changes, events, trends, successes, and failures and learn from them.
- Internal and external contexts, as well as risk criteria, which may change, and it is therefore important to adjust risk treatments and risk priorities accordingly.
- Identifying new upcoming risks.

Monitor and review assures that the process continuously incorporates new risk aspects and that the process is kept up to date.

4.3 Business Continuity Management

All risks are not known. Although the purpose of risk management is to identify risks, it is impossible to find all and analyze these, it is the whole nature of risks. Power failures, human error, industrial action, natural disasters and cyber attacks are all risks with the potential of seriously disrupting business organizations. With respect to disruptions caused by such events it is imperative that organizations have implemented systems to ensure ongoing business. BCM is relatively similar to risk management but there are some differences that researchers have agreed upon. Unlike risk management where the target is to identify known risks, BCM has been developed according to (G.A Zsidisin, S. A. Melnyk, G. L. Ragatz, 2005) in order to minimize the effects of unanticipated events on the firm's ability to meet customer requirement.
Moreover, according to ISO 22301:2012 will BCM systems help organizations indifferent of size, location or activity to be better prepared and more confident managing any type of disruption. According to (HM Government), BCM is constituted by the following steps:

- BCM programme management.
- Understanding the organization.
- Determining BCM strategy.
- Developing and implementing BCM response.
- Exercising, maintaining and reviewing BCM arrangements.

These steps are the core of BCM and a necessity in order to ensure a well functioning process. The different stages will now be explained more thoroughly

4.3.1 Step 1 – BCM Programme Management

There are three steps in the BCM programme management process that will ensure that BCM is established and supported within an organization.

Assigning Responsibilities
It is important that the senior management is hundred percent supportive in the start-up of BCM, without this support, it is very hard to convey any sense of ownership and value among the workforce. It is equally important that an individual person or team is responsible for managing the BCM capability. Based on this, it is recommended that senior management nominate an adequate member of the board to be accountable for the BCM, as well as appointing an appropriate number of employees with the

responsibility for taking the programme forward.

Establishing and Implementing BCM in the Organization
The management board has the responsibility to agree upon the BCM policy within the organization, which should contain:

- Scope aims and objectives of BCM in the organization.
- Activities that will be required to achieve these.

Once the policy has been agreed upon, it is the responsibility of the elected individual or team to implement it, this include:

- Communicating the programme to internal stakeholder.
- Arranging appropriate training for staff.
- Ensuring activities are completed.
- Initial exercising of the organization's BCM arrangements.

Ongoing Management
The responsible person or team has a number of activities that should be exercised on a regular basis to assure that the BCM programme is instilled in the organization and remains up to date. Activities will involve:

- Review and updated business continuity plans and related documents.
- Promote business continuity across the organization.
- Keep the BCM programme up to date.
- Manage the exercise programme.

Implementation of the three steps should thus ensure, responsibilities, objectives, promotion throughout the organization and continuous review.

4.3.2 Step 2 - Understanding the Organization

The business impact analysis is a key element and acts as the foundation from which the BCM is built. Undertaking a business impact analysis is essential and enables organizations to better understand the BCM capability.

Business Impact Analysis
The purpose of a business impact analysis is to identify and document the most central products and services and what critical activities that are necessary to deliver these. It also identifies the impact a possible disruption of these critical activities would have on an organization, as well as resources required to reintroduce the activities. The following steps are necessary in order to carry out a business impact analysis:

1. The most vital products and services which if disrupted for whatever reason will have the most serious impact on the organization should be identified and listed. The impact should be considered from two aspects for each service and product, firstly, it should be considered in terms of the organizations ability to meet objectives and aims, and secondly, how it would affect stakeholders. Furthermore, the impact on the organization should be estimated for an appropriate time interval, for instance the first 24 hours, after 48 hours, up to one week and up to two weeks.

2. An organization should after the first step be able to identify the maximum length of time or maximum tolerable period of disruption (MTPD) that a service or product can be inoperable without jeopardizing the viability of the organization, either through loss of image or financial stability.

3. At this stage the recovery time objective (RTO) is decided, which is the time central services or products would need to be continued in the event of a disruption. It is important to consider unexpected difficulties with recovery and the already established MTPD.

4. The fourth step includes listing all critical activities required to deliver key services and products.

5. An organization should determine the amount of resources needed over time in order to maintain critical activities at an acceptable level and to meet the already established RTO. Critical resources could include people, premises, technology, information suppliers and partners.

4.3.3 Step 3 – Determining BCM Strategy

An organizations products and services rely on a series of critical activities, which are identified in the business impact analysis. In order to maintain these critical activities, it is important that organizations identify actions and strategies to meet the RTO for each activity. This includes actions for mitigate loss of potential resources identified in step 5 of the business impact analysis. Naturally, there are several tactics one might take in order to secure or protect valuable resources. Potential actions according (How prepared are you) in regard to information and technology could be:

- Keep the same technology at different locations that will not be affected by the same business disruption.
- Ensure that data is kept up to date, backed-up and stored of site.
- Hold on to old equipment as emergency replacement or spares.

This list should not be seen as exhaustive, but a pointer in the right direction.

4.3.4 Step 4 – Developing and Implementing BCM Response

In order to ensure management of an incident, as well as continuity and recovery of critical activities, which products and services are dependent on, it is vital to have suitable response plans in place. Clearly, there is not a global response plan applicable on all sorts of organizations, these plans will vary in both content and number depending on the structure, complexity of critical activities and culture of an organization. Based on these factors, an organization may choose to implement separate incident management, business continuity and recovery plans, as well as plans covering a specific part of the organization. For a very small organization, it may be enough with a holistic plan, which contains all the above parameters. Ultimately, the key point is that an organization should be able to manage an immediate incident and recover the critical activities based on information from the established plans.

4.3.5 Step 5 – Exercise, Maintain & Review BCM Arrangements

This step ensures that the BCM plans and methods are confirmed and kept up to date. In order to verify that the BCM arrangements work they have to be exercised, if they function well, they can be considered reliable. Exercising normally involves rehearsing key staff, testing of systems that provide resilience and validating plans. There are different ways of exercising the established plans:

- A discussion-based exercise is cheap and easy to prepare. The exercise brings people together and problems or solutions to the plan can be identified. The exercise also serves as a tool for further embedding BCM within the organizational culture.

- A table-top exercise is scenario based exercise. With the exercise portraying a real life situation, decisions and actions are made much like they would in real life.

- A live exercise can be conducted in small scale or large scale. A small-scale test could be an on one component, for instance and evacuation. While a large scale test could include all components of the plan. In order for the exercise not to cause any unnecessary disruptions it is important that the organization consider the capacity needed to run it.

When the BCM arrangements are put into action it is important that a maintenance plan is put into action in order to assure that the plans are updated. Alteration of plans could be necessary when there are changes to an organization in terms of operating environments, restructuring and staff, as well as after an incident or exercise, where new information might arise.

Lastly, the BCM arrangements should be reviewed at regular intervals. The review should verify that:

- That key products and services with respective critical activities and resources have been identified.

- Plans reflect the organization's objectives.

- BCM exercising and maintenance programs have been implemented.

- Improvements identified during exercises and incidents have been included in the BCM arrangements.

A systematic implementation of the five steps will ensure that a well functioning BCM plan is in place.

4.4 Human Error

The cyber maturity is generally quite low among companies and organizations. According to PWC this is one reason why companies are trying to counter vulnerabilities and achieve digital maturity. Consequently, companies invest in technological solutions, hoping that this will do the trick and forget that security heavily relies on the human factor. A global survey conducted by PWC demonstrates that every third company educates their employees in IT security. With each infringement, organizations learn about new threats and how to eliminate them. It is easy to point out the shortcomings in technology in organizations when it is in fact the human error that is the core of many data intrusions. According to (Government technology, p. 18), 35 percent of all data intrusion can be traced to the human error. Why it is so will be further studied in this section. (PwC)

4.4.1 End Users

One of the most common ways for hackers to get into a system is through the end user. One major reason for this is the large number of end users and that security is often a limited knowledge. Phishing is the most common form of attack where regular emails look credible but actually contain malicious links or attachments. It is common for these emails to appear from a trusted sender, such as a colleague or business partner. Victims from phishing can be affected differently, ranging from a small virus infection that can easily be eliminated to ransomware that can rapidly spread across networks and infect large parts of the organization. Therefore, it is end users who are not careful and aware of the risks that can easily act as a gateway for hackers. Another problem relatable to end-users is loss and theft of hardware. People leave laptops and USB memories that often contain precious information unattended, which make them easy to steal. Also, it is common that people do not encrypt these devices. (Julie Knudson, 2018)

4.4.2 Type of Mistakes Being Made

Security mistakes occur in all organizations and they also occur at the highest levels. It is not uncommon for leaders in an organization to shift all focus on profitability, which means that security may be overlooked. One problem is once leaders and the board of directors has decided to focus on security, the budget becomes a problem. Instead of investigating what kind of security measures that are needed and construct the budget accordingly, organizations tend to allocate a small portion of the budget into security, without actually knowing if it's enough to achieve the intended measures.
Everyday mistakes are part of reality, and it happens that intrusions arise from very simple errors. Security gaps occur easily when employees are not fully committed to mitigation efforts. It is common that employees do not know what to do in order to reduce risks, and employees often have limited understanding of risks. An example of this is emails sent to the wrong recipient, depending on the content, this might compromise the security of the company. Another potentially devastating issue is when new software updates are available but are not installed in time or properly. This problem can be prevented by a more present management, which can inform the responsible person that the necessary updates must be carried out right away. This was the case of Equifax 2018. A software version constructed to handle the program that infected Equifax had been available for several months, but it had not been installed. (Julie Knudson, 2018)

4.4.3 Reducing Risk With Training

According to Government Technology, governments around the US have different ongoing training programs. Something that is common is an internal phishing campaign where employees are tested by clicking on a selection of links. The accuracy is never better than 80%, meaning 20% of all employees under a given campaign click on the wrong link. Cyber defense, in terms of assessment and awareness, is trained on routine within different states, but regardless of this, people click on malicious links and open suspicious files. The training is therefore not flawless and does not guarantee that human errors will disappear, but still has a positive effect. An example of this is, according to (government technology, p. 19-20), a vulnerable government entity that had a 20% higher victim rate than the worst state agency. By appropriate training, this figure could be reduced and compared with standard values. Since training does not completely exclude the number of errors, methods need to be developed and renewed to improve results, which can be done by:

- Keep it timely. Training modules should be constructed from recent threats in order to make them more relevant.

- Offer variety in terms of new training and testing materials in order to get the attention of employees. When the same training scenarios are offered it is likely that the employees will find it uninspiring.

A routine training drill within government agencies is a so-called 'phishing trip' where false messages with traps are sent to employees in order to see which employees that fall for it. This is a good way to analyze whether the training has any effect.

4.4.4 Back-end and Tech Fixes

Training can raise cyber security. However, the human error is inevitable and will continue to happen. Improved methods in back-end and new technology must act as a complement. IT can contribute a lot in terms of building security procedures. A simple solution that, according to (government technology, p. 20), can help, is a small warning box that pops up when a person clicks on a link. Such a box should ask if the person really wants to press the link, which means that the person has to reevaluate an extra time. Another effective way to alert people is to flag e-mails from senders outside the organization with the flag 'external'. Popular nowadays is also the use of platforms that track employee behavior patterns. These programs respond if an employee would deviate from everyday patterns, which help to reduce the number of visits to potentially harmful websites. Such programs also respond if an employee who usually log in from Stockholm suddenly log in from Poland and start performing completely different activities.

4.5 Intrusion Detection and Prevention System

Public and personal interaction is commonly carried out via wireless technology. The increasing risk for cyber attacks on these technologies make organizations vulnerable. Organizations need to stay vigilant and continue to implement new process to mitigate the chance of intrusions. Time is of the essence when an organization is attacked; detecting a compromised system or device as soon as possible is crucial. An intrusion detection and prevention system (IDPS) is able to analyze and monitor unknown signals, detect known intruder types, threats, processes and methods used and sound alarm and notifications when needed.

4.5.1 IDPS Functions

The most common way for securing wireless networks is to create or utilize some form of security mechanism. Security mechanisms often include authentication mechanisms, Virtual Private Networks (VPN) and firewalls. VPN create a safe connection between two nods in an insecure network, such as the Internet, while firewalls create a protective barrier around the network. However, these types of preventative measures are not enough for safekeeping networks around the clock. IDPS contains four fundamental security functions and can act as a complement to common security mechanisms. Functions include monitoring, analyzing, detecting and preventing suspicious activities. (Ibrahim Al-Shourbaji, Samaher Al-Janabi, 2017)

There are several ways to inflict a wireless network where the two main types are Denial of Service (DoS) and Distributed Denial of Service (DDoS). The purpose of these attacks is to overload systems and servers, making them inaccessible to others. The Difference between a DoS and a DDoS is mainly that the DDoS is a multiple connection attack, with many computers and connections, while the DoS is an attack from one

computer and one internet connection. Naturally, it is harder for a server to cope with a DDoS attack opposed to the smaller DoS attack.
Another typical attack is a wormhole attack where an attacker copies messages and packets at one location in the network and then channels them to another selected location through a worm hole tunnel, and then resends the copy into the network, making the copy arrive faster than the original.
Brute force is an attack method where attackers attempt to recover passwords and keys that are in common with all shared clients. In order to achieve this objective all possible keys are tested systematically until the right key is guessed. (Ibrahim Al-Shourbaji, Samaher Al-Janabi, 2017)

There are differences and similarities between an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS); both the systems automatically detect intrusions. The IPS can in addition to detect an intrusion also try to prevent them, as well as compare signals to already detected signals from previous intrusions and from databases containing gathered and published attack signatures. Signatures can be detected in two different ways, either by signature-based detection or anomaly-based detection.

- Signature-based detection is similar to anti-virus software that creates signatures based on attack details. When signatures have been formulated, they can be searched for in the computer systems.

Anomaly-based detection notices unusual behavior on the network or in the system. Behavior is considered unusual if it deviates too much from the agreed definition of normal. Naturally, it is important to have a credible definition of normal. The definition is often formulated through a compilation of everyday data that has not been affected by any intrusions.

Detection Technique	**Advantages**	**Disadvantages**
Signature-based	• High detection accuracy for known attacks • Low computational cost	• Low compliance for unknown threats • Difficult to keep knowledge base up to date
Anomaly-based	• Effective to detect new vulnerabilities • Less dependent on Operating System	• Time consuming to classify attacks • Activate alerts in proper time

Table 3. Advantages and disadvantages of the intrusion detection methodologies, adapted from (Intrusion Detection and Prevention Systems in Wireless Networks)

Even if an IDPS fail to prevent an attack it gathers information about the attack and how it was possible. The gathered information includes what intruders accomplished and what methods that were used in order to achieve these goals. Naturally, this information is extremely valuable to a business or organization in order to fully understand what happened, learn from the incident and reassess the current security measures.
(Ibrahim Al-Shourbaji, Samaher Al-Janabi, 2017)

4.5.2 Limitations of IDPS

There are some drawbacks with IDPS. Firstly, the system using anomaly-based detection is not hundred percent accurate, it happens that false alarms are triggered. In order to act as quickly as possible in the event of an intrusion it is necessary to monitor the alarms, which is a tiring activity since it needs constant supervision.
In order for the IDPS to run in real time it needs to stream data across the network from sensors to a central where the data is preserved and analyzed. The amount of data streamed can potentially affect the network performance. Another problem is that if the IDPS classifies a normal ongoing activity, as some type of intrusion the damage could be severe since the IDPS will try to avert or alter the activity. (Ibrahim Al-Shourbaji, Samaher Al-Janabi, 2017)

4.6 Incident Response Plan

The purpose of a cyber security response plan is to mitigate the technological, operational and financial impact of a breach. An incident response plan (IRP) should ensure that cyber threats are detected, contained and eliminated. In addition, the IRP should make sure that stakeholders are quickly informed; the severity and damage of the attack are estimated; and that systems are rapidly restored to normal function.

There are similarities between the aspects considered in an IRP to those considered when developing a BCM strategy. With the main difference that the IRP solemnly approach and manage situations related to cyber incidents and breaches. BCM, on the other hand, is a holistic management process that aims to build resilience through the organization by identifying threats and analyzing possible impacts for whatever unforeseen reason. (ISO 22301:2012)

4.6.1 Preparation

It is believed; according to (Jadhav Harsh, 2018) that hiring of external security experts that work together with the in-house team can be helpful in many cases. Experts can provide thoughts and recommendations throughout the design process. Further, it is also believed that cyber security insurance is a reasonable investment since the potential damage could be severe and a recovery process can be time consuming.

The presence of contractors and consultants in organizations is normal. However, the presence of outside personnel conveys risk. Based on this it is recommended that all contractors with access to operations should be properly examined prior to approval, during the contract and at exit, for all data integrity issues.

Preparation is about designing the right procedures and infrastructure that will support a company during an incident. Preparation should be managed like any other critical program. It is important that specific objectives, outcomes and milestones are

established. It is important to constantly study different threats and defenses, as well as test systems for vulnerabilities. IRP can have different complexity. However, a plan should at least include how events will be identified and categorized, what type of response mechanism will be used, indicators such as, RPO and MTPD should be outlined and the response team need to have established roles and responsibilities. Normally, response teams are either of centralized nature, where all incidents within the organization are reported to, or a decentralized response team with responsibility for a specific area or business unit. It is not unusual that some responsibility from the plan is transferred to a third party that can provide coverage around the clock. It is important to decide what composition of the response team. It is preferably if the team consists of representatives from management, finance and operations. Developing test plans and implement training is essential in order to raise collaboration and reduce confusion between staff, respondents and third parties on responsibilities and roles. An attack has the possibility to inhibit communication, it is therefore very important to implement a communication strategy, both an internal strategy and an external strategy for interaction with media, customers and suppliers.
Like any other program, it is important that the IRP is monitored and maintained continuously in order to ensure proper function and relevance. This include that team members with different responsibilities are reviewed regularly, as well as vendor tools and systems and applications. (Jadhav Harsh, 2018)

4.6.2 Detection

The detection phase involves identifying threats from various attack vectors and prioritizes incidents based on likelihood of occurrence and potential damage. Jadhav Harsh mentions some attacks and sources to attacks that are more common than others, which include:

- Infected flash drives
- Fraudulent web-based applications
- Brute force methods used to compromise networks through unauthorized access
- Vicious email attachments
- Users who disregard company policies by installing unapproved software

Incidents and intrusions can be detected in several different ways. Some common ways include notifications by anti virus software, changes in the system log that are unauthorized, network intrusion alarms, unusually many emails that are bounced back and irregular network activity.

4.6.3 Impact Analysis

It is important to conduct an impact analysis in the aftermath of an incident in order to understand the impact of the incident. After the impact analysis is accomplished it is appropriate to contact other entities and escalate the incident response. An impact analysis is divided into three separate steps. (California Government, p. 12-13)

Functional Impact

The functionality of an organization is threatened during an attack and the integrity, availability and confidentiality need to be investigated.

Category	Definition
None	No effect on the organization's ability to provide all services to all users
Low	Minimal Effect; the organization can still provide al critical services to all users but has lost efficiency
Medium	Organization has lost the ability to provide a critical service to a subset of system users
High	Organization is no longer able to provide some critical services to any users

Table 4. Functional Impact Categories, adapted from California Joint Cyber Incident Response Guide

Information Impact

The integrity, availability and confidentiality of information is another aspect that need to be investigated in the aftermath of an attack

Category	Definition
None	No information was leaked, disclosed, changed, delete, used or disclosed by or for unauthorized persons or purposes, or otherwise compromised
Privacy Breach	Sensitive personally identifiable information of taxpayers, employees, and beneficiaries was accessed or leaked
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information was accessed or leaked
Integrity Loss	Sensitive or proprietary information was changed or deleted accidentally or intentionally

Table 5. Information Impact Categories, adapted from California Joint Cyber Incident Response Guide

Recoverability

The amount of time and resources needed to recover after an incident differ depending on what resources that were affected and the magnitude of the incident.

Category	Definition
Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recover is unpredictable; additional resources and outside help are needed
Not recoverable	Recovery from the incident is not possible (e.g. sensitive data has leaked and been posted publicly)

Table 6. Recoverability Effort Categories, adapted from California Joint Cyber Incident Response Guide

4.6.4 Recovery

Recovery is according to the National Institute of Standards and Technology (NIST), defined as “the development and implementation of plans, processes and procedures for recovery and full restoration, in a timely manner, of any capabilities or services that are impaired due to a cyber event.”

Planning for Cyber Event Recovery
A vital part of an organizations’ preparedness to a cyber event recovery is effective planning. According to NIST the following actions are key in order to be prepared:

- Planning how the organization can continue operations in a diminished capacity. Alternatively, restore services over time based on their relative priorities.
- Document key personnel who are responsible for defining recovery criteria and assure that these persons understand roles and responsibilities.
- Create a list of processes, people, external resources and technology that are fundamental for the organization to achieve its mission, as well as categorize relative importance among the listed assets.
- Develop extensive plan(s) for recovery that support the previous asset prioritizations and use these plans to develop recovery processes and procedures that assures timely restoration of systems.
- Implement and practice the defined recovery processes.
- Define the conditions where the recovery processes will be invoked, as well as who that has the right to invoke it.
- Develop a recovery communications plan.

Execution of the above actions will ensure that an organization is in a good position before an actual cyber event takes place.

Continuous Improvement
Recovery planning is not a single time activity and plans policies and procedures created for recovery need to be improved continually. NIST argues that lessons learned, which is a post incident activity similar to postmortem analysis is a good way of achieving continual improvements during recovery efforts. Additionally, continual improvement is also achieved by validating recovery capabilities themselves. In terms of continuous improvement, NIST suggest that the following aspects are worth considering:

- Gather information concerning the recovery plans from stakeholders involved in the recovery activities.

- Formally implement cyber incident recovery exercises and tests at a frequency that is sustainable for the organization. The exercises should be realistic and include pre-determined roles and responsibilities.

- Conduct extensive post exercise debriefs to ensure that the organization analyzes and incorporate lessons learned into related plans and processes.

- Continually improve cyber incident recovery plans, policies and procedures by applying lessons learned and periodically assess the recovery capabilities themselves.

- Utilize recovery as an instrument to identify weaknesses in the organizations' processes and technologies.

Furthermore, after an incident is detected and assessed the first priority should be to contain the threat. The containment could be done in different ways depending on the threat, for instance should an infected server be taken offline as quickly as possible. Further measures could include disabling user accounts and removing infected hardware from the network. According to Jadhav Harsh it is essential to gather evidence when the instant threat has been contained. The evidence can be necessary in an investigation further down the road. It is important that the recovery effort does not manipulate any of the found evidence. The next step is to make sure that all instances of the malware are completely eradicated.

Recovery Metrics

During the recovery processes it is beneficial to collect specific metrics, which in turn may help to improve recovery and communicate continuous improvement. Metrics should be determined in advance in order to understand what should be measured and how the process of collecting adequate data should be implemented. It is also important to identify the recovery processes that are not possible to measure in an accurate and repeatable way. However, the process of collecting data must not disturb the primary task of restoring business functions. The collection of recovery of metrics should therefore be designed in a way that the metric data is an automated output from the recovery activities. The collected metrics will then be used to improve the quality of the recovery actions within the organization. The following table describes a general area to be measured together with some example metrics (NIST).

Recovery Area	Example Metrics
Assessing Incident Damage and Cost Both direct and indirect costs; recovery damage and costs may be important evidence as part of a legal action	• Costs due to the loss of competitive edge from the release of proprietary of sensitive information • Legal costs • Hardware, software and labor costs to execute the recovery plan • Costs relating to business disruption such as system downtime, For example lost employee productivity, lost sales, etc. • Other consequential damages such as loss of brand reputation or customer trust from the release of customer data
Organizational Risk Assessment Improvement	• Frequency of recovery exercises and tests • Number of significant IT-related incidents that were not identified in risk assessment
Quality of Recovery Activities	• Number of business disruptions due to IT service incident • Percent if successful and timely restoration from backup or alternate media copies • Number of recovery events that have achieved recovery objectives

Table 7. General areas to measure together with example metrics, adapted from NIST, guide for cybersecurity event recovery

4.6.5 Postmortem

After a major breach it is extremely important to re-evaluate the effectiveness of the IRP. These types of investigations and meetings should take place shortly after an incident and all relevant parties should attend, this include potential third parties. The goal of such meetings is to establish a timeline, gather facts and conduct an unbiased assessment of the incident. Included in the fact gathering process is a thorough investigation of what caused or made the incident possible, what type of obstacles were met that slowed the response process down and assessing if the procedures made by the response team followed the pre-determined rules. Further, the existing plan might be functional, but an evaluation is preferable to understand if the response team could do something different if faced with future incidents. During a postmortem meeting there are several questions that are worth addressing, these include, according to (Jadhav Harsh, 2018)

- Were the present corrective actions sufficient to deal with the incident?

- Did members of the response team clearly understand their roles and responsibilities?

- Is additional training required for users or members of the response team?

- Could better technology have uncovered the threat faster?
- What can be done to prevent or mitigate this type of threat in the future?
- Was sufficient forensic evidence obtained to satisfy any cyber security claims?

By addressing this type of questions, it will become evident what parts of the response plan that functioned properly and were improvements can be made.

Chapter 5

This chapter will portray the proposed framework. Firstly, the sources of the three-step framework are described. Then, each part will be described systematically. Each part is based on a merger between described literature and information attained from interviews and surveys.

Framework

This chapter proposes a framework that will be applicable and supportive to companies that possesses an IT infrastructure that during a potential cyber attack, can experience noticeable damage, thus preventing or disrupt the business. The model consists of three parts; (1) estimation of risks and how to minimize effects related to cyber attacks on the business, (2) how to work during an attack and (3) how the aftermath of an attack should be managed. By following the three parts systematically, companies should be able to create strategies, routines and risk mitigation measures that together provide a solid foundation for combating cyber attacks.

Part 1 Organizational Structure and Mitigation Efforts	**Part 2** Incident Response and Action Plan	**Part 3** Recovery and Postmortem
Relation to chapter 4.1-4.3	Relation to chapter 4.4	Relation to chapter 4.4.4-4.4.5

Table 8. Part headlines and relation to literature

5.1 Source of Framework

The framework is based on three main subjects, qualitative data from surveys, adequate literature and interviews with four companies from different businesses. In addition, experience gained by the author from a real life cyber incident has also influenced the framework.

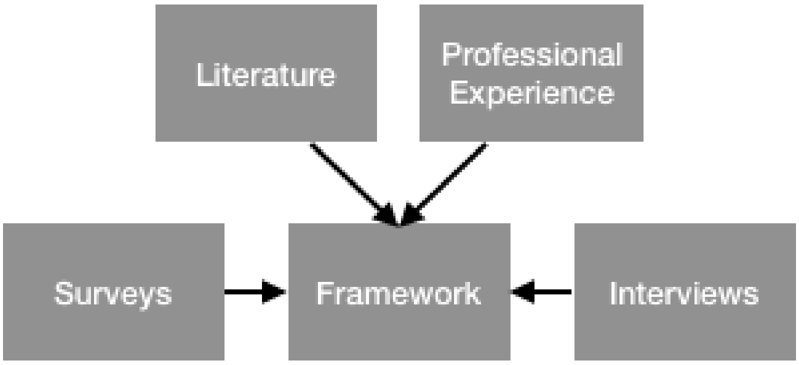


Figure 3. Sources used for creating the framework (author´s)

5.1.1 Literature

The foundation of the framework is based on academic literature. Literature covering risk management and BCM constitute the core, and previous research in the field cyber security, including scientific reports and government publications

5.1.2 Personal Experience

Personal experience from the author has influenced the conclusions drawn to a small extent. The experiences were acquired during a summer employment at a logistics and freight forwarding company, which was targeted by a ransomware attack.

5.1.3 Interviews & Surveys

Interviews have been held with four independent companies from different business areas. The businesses include, banking, manufacturing, consulting and logistics. Interviewed companies include

- Ålandsbanken – The bank is active in Sweden, Finland and in Åland.
- Yubico – The software company manufactures and sells authentication devices.
- Deloitte – The company offers a wide range of consultancy services.
- An anonymous logistics and freight forwarding company – Selling logistical solutions and services.

Surveys were sent to companies with the prerequisites of having attended the event ARKAD during the autumn of 2018, as well as having a minimum of 25 employees. It was believed to be an adequate method since surveys often have a low response rate. Out of 65 surveys that were sent out only two responded, which equals a response rate of roughly 3%. Both companies choose to remain anonyms.

- Survey1 – The company develops smart services for secure payment and information solutions.
- Survey2 – The company supplies different customer relationship management (CRM) systems.

5.1.4 Framework Overview

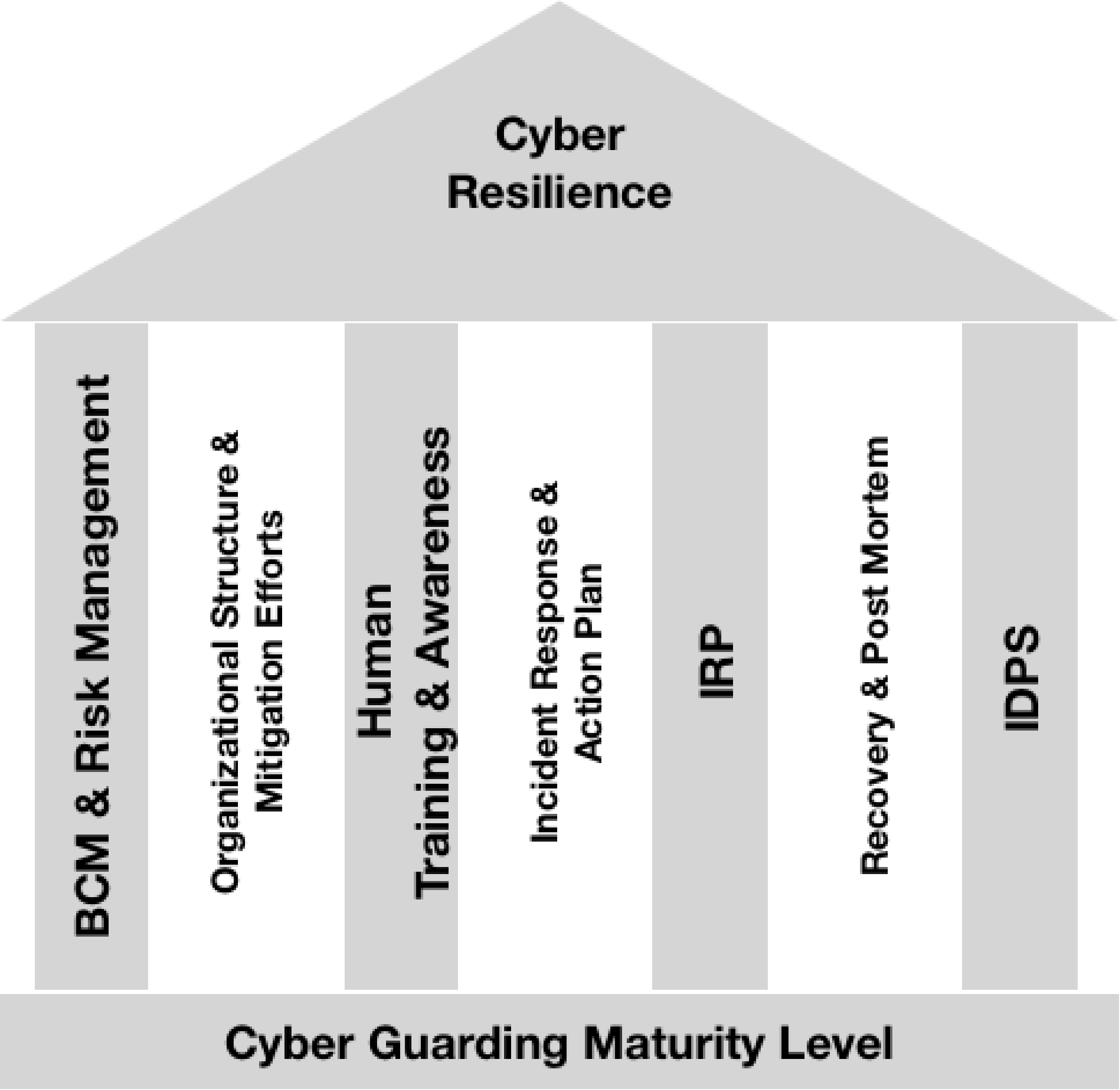

Cyber Resilience
BCM & Risk Management
Organizational Structure & Mitigation Efforts
Human Training & Awareness
Incident Response & Action Plan
IRP
Recovery & Post Mortem
IDPS
Cyber Guarding Maturity Level

Figure 4. Illustration of the correlation and structure of the framework (author´s)

5.2 Part 1 Organizational Structure & Mitigation Efforts

The first part of the framework will suggest how risks related to cyber attacks could be identified and estimated, as well as how to minimize the chance and effect of a potential attack.

5.2.1 Implement Risk Management

A risk management process needs to be implemented within the organization; this must be the first priority. This is a proven method to manage risks and is commonly used among various companies.

Firstly, the parties involved in the risk management process have to be selected and responsibilities need to be assigned. The composition of the risk management team is decided by the business unit manager or senior management and should involve at least one employee from the different functions, which then answers to one senior risk manager. Adequate information is then reported back to the business unit manager who is responsible for communication outside the business unit.

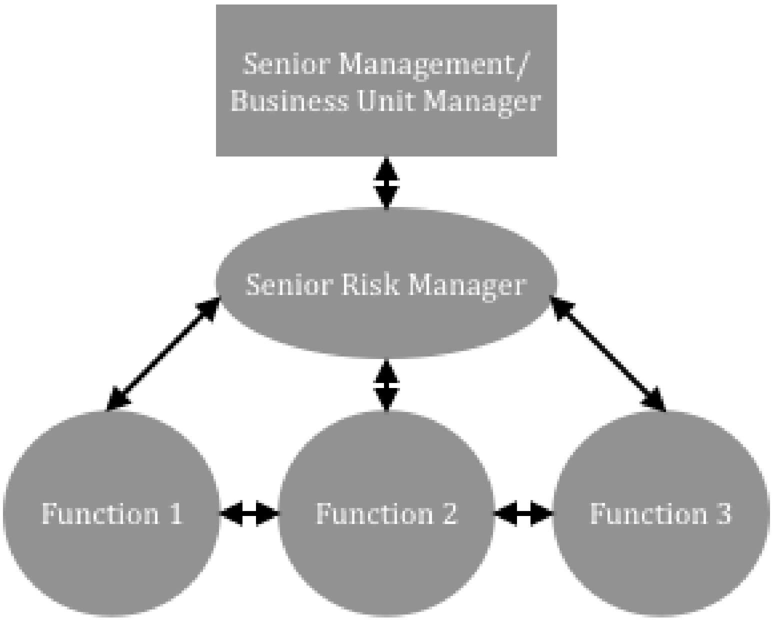


Figure 5. Involved parties and the structure of the risk management team (author´s)

Secondly, the context of the organization needs to be decided. It is important to understand the objective, goal and the operating environment of the organization, which risks need to be managed in harmony with. It is vital to understand what is really important to the company. For instance, if the business unit handles a large number of personal information, it is crucial that this information remains safe and unexploited. The business unit might rely heavily on server operability; if the server were to be inaccessible it would directly damage the company since customers will not be able to buy products. This is the case for Survey1. The company divides cyber threats into two categories, firstly, information leakage where perpetrators attempt to attain sensitive information. And secondly, attempts to make servers inaccessible, mainly through DDOS attacks.

Another aspect of great importance is the internal coherence of the organization. It is vital to understand how the organization is structured since this will affect the flow of information and how strategic decisions are made. Focusing on IT, it is important to understand where decisions are taken and who is responsible. Are decisions made from a centralized position and channeled down through the organization or from a decentralized position, with each business unit responsible, independently of one another. Further, declared in the introduction, this framework assumes a decentralized position where business units act independently of one another.

Risk identification is an important process and aims to find, recognize and describe different risks. When the risk management team has understood the context, objective and the essentials for doing business within the unit a brainstorm session is in order. Brainstorming is the most effective method to identify risks and observe the viewpoint from the whole team. During the meeting the risk management team tries to identify relevant risks and threats in line with the organizational objectives and goals.

Risk Library

Identified risk need to be stored in a risk library. According to Ålandsbanken a risk library is a folder where risks and threats are described and stored. The library is accessible to the whole organization. The risk management team needs to assign each identified risk with likelihood and corresponding severity/consequence according to the risk heat map discussed in chapter four. This will assure that each unit and employee is kept up to date and understands recent identified risks. The senior risk manager is responsible for reviewing the library and keeps it updated by reevaluating current risks, adjusting the heat maps and descriptions, as well as identifying new emerging risks and threats.

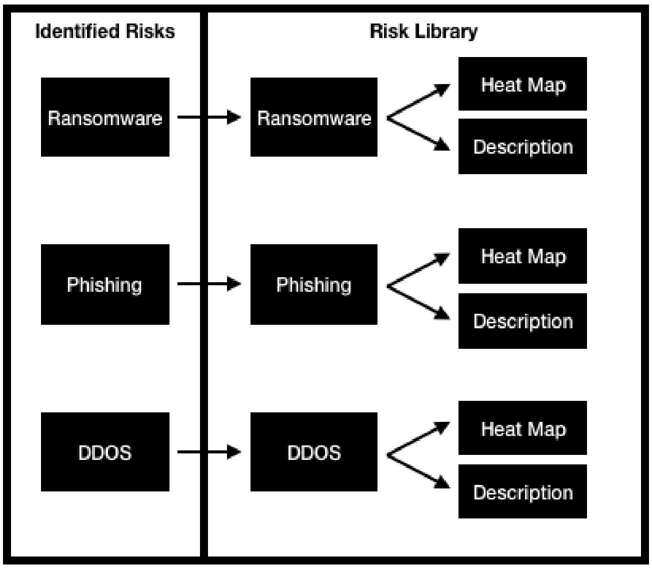


Figure 6. New risks and threats are identified and stored in the risk library (author´s)

Author´s library provides a holistic view of risks, which the organization needs to be aware of. The next assignment for risk management team is to evaluate these risks and determine from their perspective, which are tolerable, and which are more significant and could potentially cause great damage. Risks deemed significant need to be treated in the best possible way, which the team will decide upon. Appropriate precautionary and preventative measures need to be installed which will be discussed further in this chapter.

5.2.2 Implement BCM

BCM is an important programme and gives organizations the best possible prerequisites to manage disruptions caused by any exterior factor. BCM has a lot in common with risk management, with the main difference being that BCM concentrate on how to deal with identified risk if they were to be realized.
It is vital that a BCM programme is implemented and the senior management is responsible for developing the BCM structure, which resembles the structure for risk management. Management needs to appoint an adequate member of the board to be accountable for the BCM programme along with a suitable team to drive the programme forward.

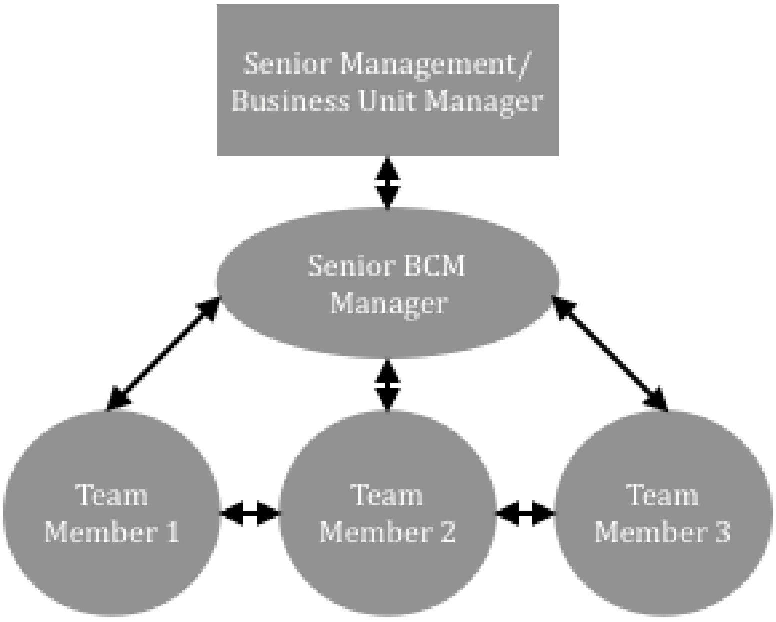


Figure 7. Structure of the BCM programme (author´s)

IRP
An IRP plan is another programme, which has a specific focus on breaches in the IT milieu. It differs from the BCM in that aspect, since the BCM has a more holistic approach. The IRP should ensure that cyber threats are detected, contained and eliminated. In addition, the IRP should make sure that stakeholders are quickly informed; the severity and damage of the attack are estimated; the spread of the undesired program or code is limited and that systems are rapidly restored to normal function.

A decentralized response team with responsibility for each business unit needs to be formed. The senior management/business unit manager decides which representatives that are deemed appropriate for the response team, which preferably consists of representatives from management, operations and finance. For instance, the interviewed company Yubico has this resource in-house and there is someone with responsibility around the clock, ready to act when situations arise. Not all organizations possess the necessary resources or competence to manage an IRP.

Some responsibility or the entire plan should then be transferred to a third party that can provide coverage around the clock. Test plans and drills need to be developed and executed in real life in order to reduce confusion and integrate collaboration between staff, respondents and possible third parties.

During an incident and when help is required from third parties it is extra important to be careful. According to Deloitte the security and supervision of third parties on site is sometimes defective. It would not be too difficult for an imposter to gain access to computers and networks by claiming to be an employee of the third party. It is therefore imperative to be mindful when outsiders are brought in. If an employee feels unsecure about someone, simple things like checking ID and getting positive confirmation from the third party is helpful. Also, the logistics provider suggests that external consultants receive limited access and when their work is done it is important to erase the temporary users.

5.2.3 Training and Spreading Awareness

Organizations need to become vigilant and careful concerning IT. All employees have to understand that the smallest of things can have major consequences. In order to instill this way of thinking, training and spreading awareness is essential.
In order for the education to be as efficient as possible it need to inform new employees as quickly as possible. Also, the education has to be ongoing in order for employees to rehearse and understand new threats. Lastly, secret campaigns should be introduced, testing employees on specific threat recognition.

Education for New Staff

New staff should attend an informational lecture sometime during their first month. The lecture ends with a summarizing test that needs to be passed. The lecture is held by an appropriate member of the risk management team and should cover

Information about attacks that are more common than others, this include:

- Infected flash drives
- Fraudulent web-based applications
- Brute force methods used to compromise networks through unauthorized access.
- Vicious email attachments
- Ransomware
- Phishing
- Yubico and Ålandsbanken also emphasizes the importance of understanding social engineering, were employees are misled. An example of this is modified emails that look like they are sent from the CEO, which demands sensitive information or payments.

The lecture should then continue with information about inconsiderate behavior that could lead to a breach, including:

- Users who disregard company policies by installing unapproved software.
- Point out the importance of contacting the senior risk manager first if something suspicious appears and await instructions.
- If uncertainty arise concerning numbers appearing in emails or invoices it is better according to Yubico to check with finance or looking up numbers manually.
- Stress the importance of not leaving personal hardware unattended, and not encrypting USB memories and laptops.

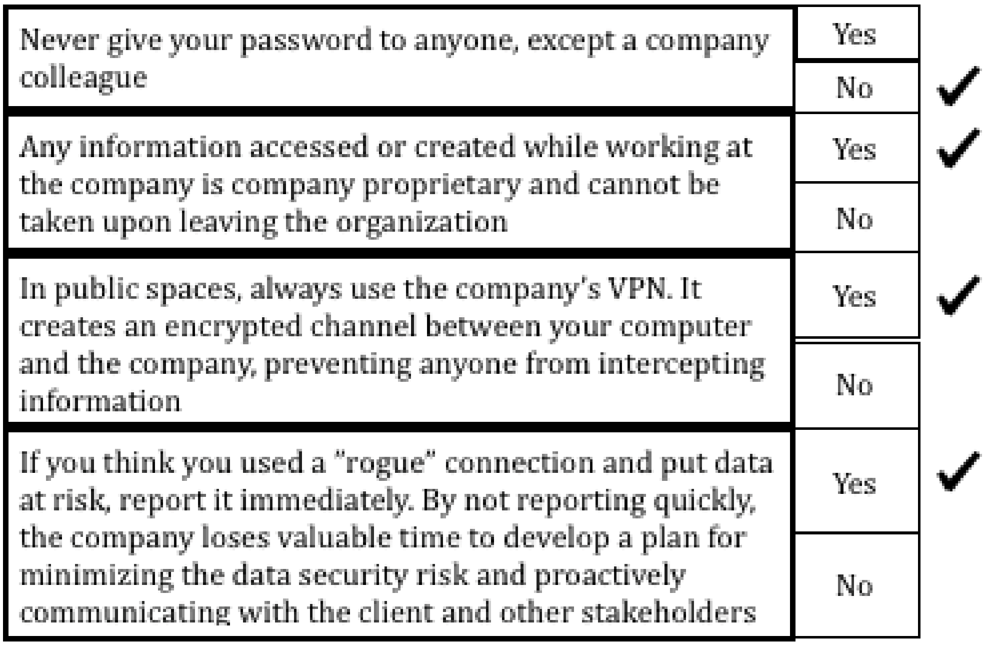
Round of the lecture with a demonstration of the software center, which will be explained in more detail in the next section, shedding light on:

- The interface of the software center and what type of software is available.
- Explain that it is not possible to download software from elsewhere and why.

By going through this lecture, the awareness and knowledge of employees will be improved.

Ongoing Tests

Both the logistics provider and Deloitte undertake test in order to maintain focus and awareness, and it is recommended that all employees take online test every sixth month or when it is deemed necessary. The following picture will show how a portion of such test could be shaped.



Never give your password to anyone, except a company colleague	Yes	
	No	✓
Any information accessed or created while working at the company is company proprietary and cannot be taken upon leaving the organization	Yes	✓
	No	
In public spaces, always use the company's VPN. It creates an encrypted channel between your computer and the company, preventing anyone from intercepting information	Yes	✓
	No	
If you think you used a "rogue" connection and put data at risk, report it immediately. By not reporting quickly, the company loses valuable time to develop a plan for minimizing the data security risk and proactively communicating with the client and other stakeholders	Yes	✓
	No	

Figure 8. Question examples for ongoing tests (author´s)

Another reliable way for spreading awareness according to the logistics provider and Ålandsbanken is through the intranet. The risk management team decides what should be shared on the intranet; this should include information about the ongoing work of the risk management team and current circulating threats.

Secret Campaigns
A great way to test whether the ongoing test and education has any effect is to conduct secret campaigns. These campaigns need to reflect real and current threats. For instance, a series of fake messages with malicious links are sent to employees to see who take the bait or acts of protocol. It is the responsibility of the senior risk manager to develop these tests and make sure that employees who act wrong are notified and lectured.

5.2.4 Back-end Technology and Monitoring

There are clever ways to limit options for employees and make one think an extra time before opening an email or entering a specific web page. It is recommended that plug-ins are installed, which will contribute to the following:

- Emails that arrive from outside the organization will automatically be marked with "EXTERNAL". When these emails are clicked on, an additional box will appear with a question if the alleged person wants to continue.

- A collection of work related web pages have to be established. This is helpful according to the logistics provider when someone tries to enter a site outside the pool. When this happens, a box will pop up and inform the employee that the site is not work related and ask if one want to continue. Additionally, it is wise to completely ban sites with suspicious content.

The logistics provider and Deloitte stress the importance of implementing a software center. Programs and software can only be downloaded from here and it is impossible to install software of any type that has not gone through a quality control in the software center. Programs that are uploaded in the center have to be thoroughly examined and approved. Utilization of a software center thereby eliminates the risk of having harmful programs and software downloaded.

Furthermore, programs identifying behavior anomalies are advantageous to have. An example of this is software that reports back if a user that usually log on from Stockholm log on from another country performing a suspicious or uncommon set of activities.
In addition, Yubico highly recommend the use of an agent that track what processes that runs on a unit. It should be installed on all company units and before one can log in on a unit the agent must inform that it recognizes all process. This is an efficient precaution to prevent malicious programs getting access to company systems.

Most companies nowadays use some sort of two-phase authentication and it is recommended to implement such precaution. Common among companies is the use of an authentication code wired through the mobile in order to get access.
Yubico, which operates in this field has developed a key, called yubikey. This key enables two-factor, multi-factor and password less authentication with physical interaction from the user, which makes it near to impossible to gain unauthorized access.

Passwords with low security in customer environments are according to Survey2 their main threat to their business. Furthermore, Deloitte acknowledge this problem and informs that most passwords contain the alleged person's name, middle name or something similar followed by a set of numbers, normally 123. An experienced hacker or programmer cracks these types of passwords easily.

Another type of monitoring, which according to Yubico is extremely important is software that logs activity. This is used to gain supervision of activity and to facilitate work in the aftermath of a breach. Every time something is changed or saved it is possible to see who made the changes, at what time and why.
Yubico continues, it is equally important to save traffic in and out from the organization for at least two weeks back in time. By comparing saved traffic with logs makes it easier to understand what went wrong and how a breach was possible.

5.2.5 Layer Security

The logistics provider has lately restructured their IT infrastructure. From a lack of protective barriers and a global IT system, a transformation towards a more independent structure has taken place. Both Ålandsbanken and the logistics provider believe that encapsulated business units with independent IT systems and networks will limit exposure of possible malicious program to spread. Ålandsbanken stresses the importance of carrying out new updates, which mostly is an automated process, as well as scanning the milieu regularly for weaknesses. It is recommended to bring in an external part to scan the milieu monthly in order to attain an unbiased evaluation. Further, according to Ålandsbanken each business unit need a security structure constituted by different layers. Naturally, this structure will differentiate depending on resources and size of business units. However, the layers must include

- Firewall protecting the network.
- Anti virus software
- Assurance that applications, programs and operating systems are running on the latest version, which according to the logistics provider is taken care by the software center which automatically pushes out updates.
- The logistics provider also emphasizes the importance of assuring that there are no servers running on unsupported operating systems.
- If resources exist, bring in third parties to scan the milieu for weaknesses.
- If it is possible an IDPS is very useful. However, according to Yubico it is a question about resources, both financial and staffing. There has to be someone looking after the system and making sure that it is updated. Otherwise referring to IoT, it becomes like any other system that runs on late versions, a weak link and a potential access point.

By implementing this list of preventative measures together with a trained and aware staff will result in a resistant structure. The picture presented on the next page demonstrates the different layers. The firewall is the outermost layer and the human firewall is the inner layer. However, the layers are all equally important and function as an entire unit.

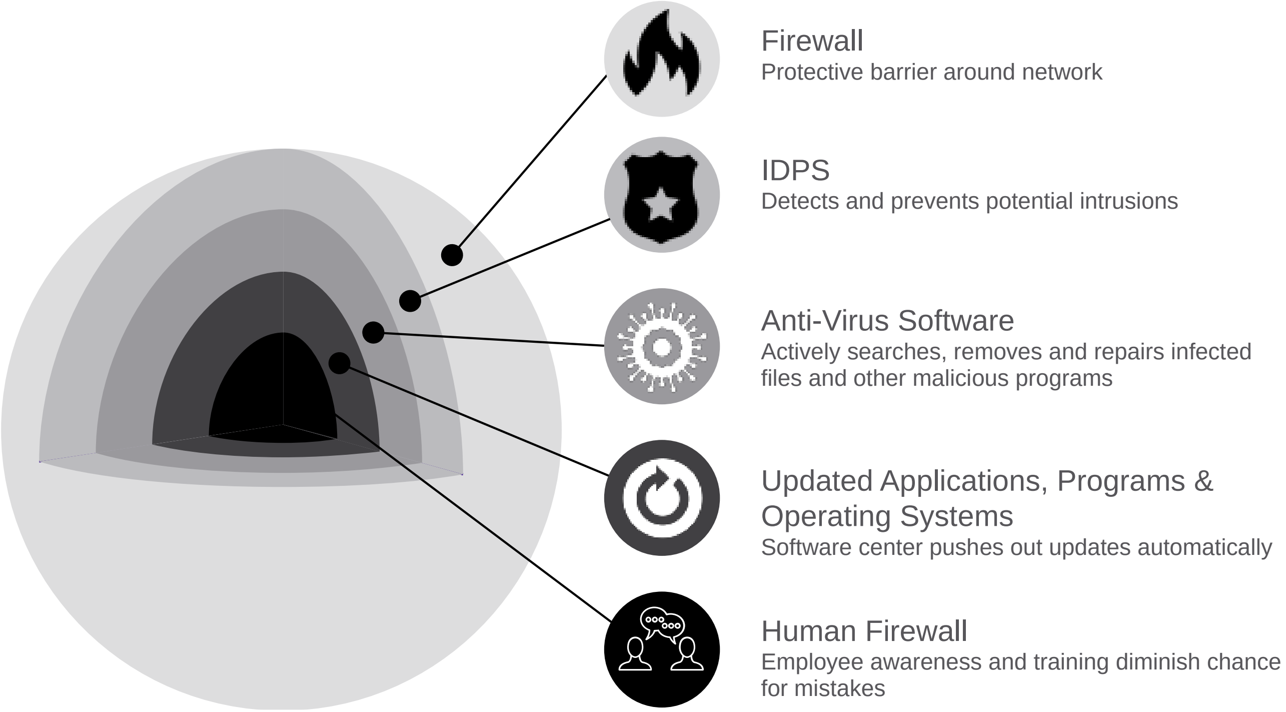

Firewall
Protective barrier around network
IDPS
Detects and prevents potential intrusions
Anti-Virus Software
Actively searches, removes and repairs infected files and other malicious programs
Updated Applications, Programs & Operating Systems
Software center pushes out updates automatically
Human Firewall
Employee awareness and training diminish chance for mistakes

Figure 9. Security structure with different protective layers (author´s)

5.2.6 Back-up Data and Insurance

Among the interviewed companies there is a general consensus that back-up data is a necessity in order to restore company operability, files and data in an effective manner. All back-ups need to be stored outside the internal milieu in order to assure that the backups do not get compromised by a potential breach. It is recommended according to the logistics provider that back-ups are taken daily from file servers. Further, essential IT systems that not lies in the internal milieu also need to be backed up so there always is available data if something were to happen at the external suppliers

Yubico has developed a hardware security (HSM) key that enables secure storage of sensitive data and information. For instance, the root to all security for a bank has to be stored offline since the server can be hacked. These secrets can then be stored on the HSM key; even if the server got hacked it is impossible to attain the secret key on the HSM. Further, Yubico recommends that files are backed up daily and refers to problem of ransomware, which encrypt files. Therefore, it is important to have an updated copy.

Insurance related to damage caused by cyber attacks and breaches is vital to have and according to interviewed companies it is a viable investment. Especially because it is hard to estimate the potential damage a breach can have on an organization.

The main areas covered in this part are presented in table 9 below:

Part 1
Risk Management
Business Continuity Management
Training and Spreading Awareness
Back-end Technology and Monitoring
Layer Security
Back-up Data and Insurance

Table 9. Key topics from part 1

Organizations should achieve great cyber resiliency by adapting the introduced models and recommended efforts in a suitable manner from each section presented above.

5.3 Part 2 Incident Response and Action Plan

The second part will cover how an organization should act when an attack or a breach has occurred. It is imperative that an organization has a plan to deal with the threat as quickly as possible in order to avoid confusion and to get the situation under control.

5.3.1 Impact Analysis

The first thing an organization need to do when it has been attacked or inflicted with unknown programs is an assessment of the situation in order to understand what type of threat there is and the magnitude of the problem. Ålandsbanken suggests that the organization find out how many computers are affected, is it one computer or is it one hundred, and make further decisions based on that. This action resembles the functionality impact, which is first step of the impact analysis.
Further, it has to be determined if any information was leaked or disclosed and from what information category. Lastly, an estimation of the recovery time has to be established and if additional resources plus external expertise are needed.

5.3.2 Communication & BCM Applicability

Concerning internal communication, the logistics provider emphasizes the importance of addressing the employees quickly of the problem through a meeting, as well as making sure that employees do not do anything without the permission of the senior management. Examples of this include not restarting any servers, connecting additional units to the network and discussing the situation with people outside the organization.

Further, the logistics provider and Ålandsbanken mentions that during an incident the BCM program is very helpful and it is therefore important to have a well structured, organized and rehearsed BCM program. Ålandsbanken also mentions that financial institutes have special requirements concerning business continuity plans, specified by the licensing authority. Furthermore, Yubico point out the importance of a BCM program and recommend that the program is designed for one year ahead in time and that regular meetings are held to possibly review it.

5.3.3 Secure Milieu, Secure Evidence & Eliminate Threat

If a large number of computers are affected and the functionality is significantly worsened or if malicious programs/viruses has been detected, Survey1 argue for a complete shutdown of the milieu and disconnecting the infected network. However, if the magnitude of threat is of smaller nature and can for instance be narrowed down to just one infected computer it could be enough to take this server offline as quickly as possible.

When a threat has led to a shutdown of the milieu, the milieu has to remain like this until the problem has been identified. At this point the IRP has to be amped up. As Yubico mentions, it is vital that someone in the response team is available at all times, including weekends and holidays. As a suggestion, a hotline between all team members is established and at least one need to be on duty for initial contact following a rolling schedule. Once contacted, the response team needs to meet as quickly as possible and gather necessary resources to identify and map the problem, which may include third party expertise if the resources do not exist within the organization.
Once the problem has been identified it is important that potential evidence is secured. This is in order to facilitate the work of the authorities if a crime has been committed.

According to Yubico it is wise to budget for extra hardware that can be used to copy hard drives, which can be decisive in order to satisfy any insurance claims. Once evidence has been secured the response team need to initiate rehearsed recovery processes and restore the system functionality and make sure that the threat is eradicated from the infected servers, as well as scan the viability of the network.

The essentials covered in this part is presented in table 10 below:

Part 2
Impact Analysis
Communication & BCM Applicability
Secure Milieu and Evidence
Eliminate threat

Table 10. Key Topics from part 2

The actions and guidelines presented in the sections above are recommendations that should be implemented and exercised to limit damage during a potential intrusion.

5.4 Part 3 Recovery and Postmortem

The last part will throw light on recovery planning and what organizations need to focus on in the aftermath of an attack, when the threat has been eradicated and when the functionality of processes and systems are restored.

5.4.1 Recovery Planning, Continuous Improvement and Metrics

The recovery process in the aftermath of an attack is naturally very important in order to ensure that stability and function is restored in the best possible way. However, to do this, it is equally important to take the right planning efforts. With good planning the whole recovery process will become easier to execute and become more effective. Furthermore, the aspect of continuous improvement of the different recovery process in place is also very meaningful. There is consensus between the interviewed companies in a number of aspects raised by NIST and it is advisable to implement procedures from the areas of both planning and continuous improvement, which are summarized in the following table.

Planning	**Continuous improvement**
• Planning how the organization can continue operations in a diminished capacity. Alternatively, restore services over time based on their relative priorities	• Gather information concerning the recovery plans from stakeholders involved in the recovery activities.
• Document key personnel who are responsible for defining recovery criteria and assure that these persons understand roles and responsibilities	• Continually improve cyber incident recovery plans, policies and procedures by applying lessons learned and periodically assess the recovery capabilities themselves
• Create a list of processes, people, external resources and technology that are fundamental for the organization to achieve its mission, as well as categorize relative importance among the listed assets	• Conduct extensive post exercise debriefs to ensure that the organization analyzes and incorporate lessons learned into related plans and processes
• Develop extensive plan(s) for recovery that support the previous asset prioritizations and use these plans to develop recovery processes and procedures that assures timely restoration of systems	• Formally implement cyber incident recovery exercises and tests at a frequency that is sustainable for the organization. The exercises should be realistic and include pre determined roles and responsibilities
• Define the conditions where the recovery processes will be invoked, as well as who that has the right to invoke it	• Utilize recovery as an instrument to identify weaknesses in the organizations' processes and technologies
• Develop a recovery communications plan	
• Implement and practice the defined recovery processes	

Table 11. Aspects to consider when planning and improving a recovery processes, adapted from (NIST, guide for cybersecurity event recovery)

In order to improve recovery processes and communicate continuous improvement it is recommended that measurable metrics are introduced. The metrics need to be determined before an incident and should help to create an overview and understanding of which area(s) of the organization were improvements can be made. It is important that the collection of data does not interrupt the recovery processes itself, but instead silently gathers data through automated processes where the metrics are the output from the recovery processes. Depending on organization the recovery areas can be altered in order to fit their preferences and interests, as well as the ancillary metrics. The table below should therefore be seen as a guide:

Recovery Area	**Example Metrics**
Assessing Incident Damage and Cost Both direct and indirect costs; recovery damage and costs may be important evidence as part of a legal action	• Costs due to the loss of competitive edge from the release of proprietary of sensitive information • Legal costs • Hardware, software and labor costs to execute the recovery plan • Costs relating to business disruption such as system downtime, for example lost employee productivity, lost sales, etc. • Other consequential damages such as loss. of brand reputation or customer trust from the release of customer data
Organizational Risk Assessment Improvement	• Frequency of recovery exercises and tests • Number of significant IT-related incidents that were not identified in risk assessment
Quality of Recovery Activities	• Number of business disruptions due to IT service incident • Percent if successful and timely restoration from backup or alternate media copies • Number of recovery events that have achieved recovery objectives

Table 12. Example of recovery areas to be measured, adapted from (NIST, guide for cybersecurity event recovery)

5.4.2 Post Mortem Meetings

In the aftermath of an incident it is of interest for the affected organization to find out what made the incident possible and how the response mechanism function. According to Survey1 it is a necessity to review the security protocol in order to understand if there is anything that can be handled better the next time. A proven method to evaluate the incident management is in the form of a post mortem analysis, which Survey2 always conduct after a major incident. Meetings should take place shortly after an incident and all relevant parties should attend, this include potential third parties. The existing plan might be functional, but an evaluation is preferable to understand if the response team could do something different if faced with future incidents. Questions worth addressing include:

- Were the present corrective actions sufficient to deal with the incident?
- Were any actions taken that might have obstructed the recovery?
- Did members of the response team clearly understand their roles and responsibilities?
- Is additional training required for users or members of the response team?
- Could better technology have uncovered the threat faster?
- What can be done to prevent or mitigate this type of threat in the future?
- Was sufficient forensic evidence obtained to satisfy any cyber security claims?

Further, Deloitte also verifies the importance of evaluation of incidents. Deloitte practices lessons learned, which is a post incident activity similar to postmortem analysis. Complementary actions to identify the root cause could include:

- Reviewing of logs, which according to Yubico is the most paramount in order to understand what happened.
- Determine if the incident caused damage prior to detection.
- Determine if the actual cause of the incident was identified.
- Determine if the incident was a recurrence of a previous incident.

By addressing these questions, it will become clear where the problems lie and adequate measures can be taken in order to cope with them, which for instance could include increased training due to confusion, reevaluate members in the response team and invest in better detection technologies. When an action plan has been created to mitigate and minimize the effect of future events it is crucial that the senior management make sure that the plan actually is attended to, which according to Ålandsbanken often is something organizations have problems with.

5.4.3 Test Milieu

When sufficient measures have been taken and the action plan has been fulfilled and implemented, the milieu needs to be properly examined and tested, preferably by a third party in order to avoid biased assessments. In parallel to third party investigations the organization should conduct internal evaluations as well. The work following an attack is an iterative process, were continuous assessments are undertaken from two perspectives, from the third party and internally in order to understand how altered or newly implemented actions function. By initiating an iterative test process, the established measures are tested and if they don’t function as intended and weaknesses are identified, the measures need to be evaluated, changed and tested all over again. This has to be done until desired effect is achieved.

Introducing different attacks and malicious programs that recently penetrated company barriers to the IDPS, firewalls and the virus protection software is a way to test the effectiveness of the milieu.

In order to understand who hacked the organization and what happened Yubico refers the importance of logging activity. This includes internal activity such as logging when and why changes are made, as well as logging traffic in and out of the organization. Comparing these logs is key in order to take the right precautionary measures. Many times, the organization doesn’t understand what happened and simply reinstalls all the servers. It is then likely that the attackers will come back and use the same penetrating strategy, but this time do it more silently and thus evade detection.

The highlighted areas in this part are presented in table 11 below:

Part 3
Recovery Planning
Continuous Improvement and Metrics
Exercise recovery processes
Post Mortem Meetings & Evaluation
Test Milieu

Table 13. Key topics from part 3

The efforts described from each topic presented above are actions to consider in the aftermath of an attack and finalize the process of combating cyber attacks.

5.5 Framework Summary

In this chapter the author has presented a framework for combating cyber attacks and intrusions. The framework is divided into the parts and since it is believed that organizations are victimized independent of business area the framework is intended to be applicable for a variety of organizations.

The first part covers how one should estimate and identify risk related to cyber threats, mainly through the processes of risk management and BCM. It also introduces procedures and guidelines to undertake for mitigate the chance and effects of a potential intrusion, for instance by implementing training efforts, different security layers and back-end technology.

The second part continues with actions organizations need to undertake during a potential attack. It covers what type of analysis that needs to be done, the importance of communication and how the IRP should function in order to secure the milieu.

The final part addresses important aspects to consider in the aftermath of an attack. Including how recovery planning is a continuous improvement process, which needs to be exercised and evaluated before and after a potential breach. Further, the part also emphasizes the significance of post incident meetings to assess the entire recovery process in order to make it more effective and identify improvements.

Chapter 6

The last chapter will tie things together with a conclusion of the framework. Then, reflections regarding the influence of the problem delimiters are reviewed, and whether the project objective was reached. Finally, the academic contribution of the thesis and future research is discussed.

Reflections

6.1 Framework Conclusions

Through the process of creating the framework, deepening my knowledge in the area of cyber security and discussing the subject with knowledgeable company representatives it has become evident that cyber security is problematic and need to be addressed from various viewpoints. It is very hard to know what to look out for, since new methods of cyber attacks and threats are constantly developed, and existing methods are tweaked in order to satisfy the demand of villains. In order to attend to this problem companies nowadays spend more resources on knowledgeable employees and high-end security programs and processes. All of these resources, which constantly need to be supervised, updated and developed in order to protect against the ever lurking cyber threat.

In order to stay ahead of the problem, it is immensely important that organizations are prepared for the worst. The framework suggests a series of programs and planning procedures, which need to be implemented in order to stay in front.
Firstly, all businesses are different, and therefore the individual risks and threats might also be very different. In order to identify threats and risk companies are recommended to use the risk management program, which is a proven method and also very popular among the interviewed companies.

When risks are identified, companies need to implement procedures and planning efforts to ensure continuity if these risks were to be realized. The framework suggests that companies implement and work with the BCM program. The program is a comprehensive and reliable program that will ensure continuity for a major of unforeseen threats and risk that might cause disruptions. The interviewed companies, all work with this to some extent and the program acts as the foundation in their business continuity processes. Another important part in the planning phase is the recovery planning. In the recovery planning organizations need to list technology, processes, people and external resources that are fundamental for the organization and develop recovery processes for these assets based on the relative importance. Further planning actions include how the organization can continue in diminished capacity, development of a communications plan, and practice the defined recovery processes.

After the above-mentioned procedures and planning efforts the framework continue to discuss the importance of employee training and spreading awareness among the organization. The imminent threat from cyber criminals will always be present and they often succeed with their crimes, where human errors often are the point of entry by unwillingly or knowingly inviting attackers. This framework has assumed that errors are made unwillingly, but naturally there are cases were employees are involved and knowingly assist attackers. However, all cyber crimes cannot be blamed exclusively on human errors. One explanation to the increasing success of cyber criminals could simply be that they are very skilled and are able to penetrate company barriers through methods and channels previously unknown to the company. Another reason could be technological flaws or discontinuities, for instance in company servers, which, in the prolongation for some cases can also be traced back to human errors in terms of manufacturing errors. Human errors have greatly influenced the framework, mainly since this is one aspect that is controllable in terms of training and by instill a working state of focus, accuracy to detail and carefulness. The framework suggests that, by continuously working with the organizations' staff the risk of being targeted by cyber attacks should be reduced. The aspect of human errors is acknowledged by the interviewed companies, which work with their colleagues in different ways. It is common with some sort of online testing and introductory training courses, which has been implemented in the framework in additions to secret campaigns.

In light of this, the framework covers a series of precautionary measures that are meant to make employees think twice and stay alert. Further, the framework proposes protecting security technologies, for instance the usage of IDPS is recommended. This particular type of technology is quite expensive and resource demanding, and it is therefore up to each organization to assess their situation and implement technologies like this accordingly. However, if resources exist, IDPS is recommended and its one of the pillars in the presented layer security structure. The other pillars, which can be considered mandatory are, firewalls, virus programs, keeping programs, applications operating systems up to date and, finally, the human firewall.

Considering the IRP, which can be seen as an extension to the BCM program, the plan includes that threats are detected, contained, eliminated and that processes are restored to normal function. The response plan is invoked during predetermined conditions and the responding team needs to assess and map the problem and gather necessary resources. Further, the team also needs to initiate the recovery process previously defined and exercised during the recovery-planning phase. The recovery process is important in terms of gathering information, as well as using it as an instrument to identify weaknesses in technologies and processes.

The recovery process needs to be improved continuously by implementing lessons learned and companies are also recommended to conduct thorough post mortem analysis of the entire incident. There is consensus between the interviewed companies that this is crucial part in order to obtain a holistic view of what made the incident possible, if the existing actions were sufficient to deal with the incident and what can be done in the future to ward of similar threats.

6.2 Influences by Delimitations

Projects of these types are often in need of some type of problem delimiter. Delimiters are established in order to make a problem manageable. This can be done by assuming and disregarding certain aspects of the problem. For this thesis the problem delimiters were created in such a way that the created framework would be holistic and applicable for a wide range of organizations. Delimiters implying this are for instance:

- Companies are targeted indifferent of size and business area.
- The framework should be applicable for organizations with a number of employees ranging from 25-1000.
- The framework is intended to be applicable for each business unit in large organizations, and for smaller organizations, which may only have one or two units.

The above delimiters with their holistic approach have contributed to an open door, and it has been possible to collect qualitative data from a wide range of companies through both surveys and interviews, which made things easier. In relation to focusing on companies from a specific business area with a turnover between 100-500 million Swedish crowns making the selection much scarcer and sought information may not have been able to attain. Additional delimiters specified in chapter 1 are:

- The framework will not focus on specific intrusions or attacks.
- Attacks are initiated externally and from unknown initiators without intentional help from the organizations' employees.
- Decisions and actions can be taken on site without confirmation from central management.

The framework will not focus on specific intrusion or attacks, but instead suggest a general approach. This also entails a holistic approach and because of this, there is no need to describe all the different attack patterns/methods in detail. This would have been too time consuming and rather difficult since the attacks and methods are quite complex and hard to fully comprehend. On the other hand, this could have been an alternate approach to the project, where the framework revolves around a specific threat, for instance ransomware, with a specific framework.

That attacks and intrusions are initiated from outside company barriers and without intentional help from employees is an assumption, which should reflect the reality quite well. Naturally there are cases where employees are the initiators and the attackers. However, this aspect is disregarded since this is hard to map out and difficult to understand why and when employees would defraud the alleged company.

The last delimiter, which implies that decisions and actions can be taken on site is there to simplify the complexity of organizations and thus enabling analysis of larger companies, which often is constituted by many business units in different countries. In reality, business units connected to large organizations are commonly dependent on central management in important questions concerning company strategy.

6.3 Completion of the Project Objective

The objective of this thesis was to create a three-step framework for managing/monitoring attacks on the IT infrastructure of companies that can suffer severe damage from a cyber attack/intrusion.
The first part where the framework should propose actions to estimate risks and minimize effects related to IT-attacks is covered by programs like risk management and BCM, as well as actions including training, back end technology and layers security.

The second part treat how organizations should act during an attack by explaining concepts of impact analysis, communications and how the IRP should operate.

The goal of the third part was to explain how an organization should work in the aftermath of an attack. The goal is reached by describing how companies need to work with post mortem analysis, planning ahead and finally iteratively test milieus to achieve desired effects.

Thus, with all things considered, the objective of this project is reached in all aspects. The framework is structured as intended and suggests methods, models and actions organizations should implement in order to create resiliency and combat cyber attacks.

6.4 Contribution to Science

Cyber security is a fairly new topic and has really gained the attention it deserves the last 20 years. Therefore, the area is not rich in literature compared to for instance, supply chain risk/management. Also noteworthy is the permanent change this area experience, with constant introduction of new technologies and methods to circumvent security. The literature and research are therefore in some sense perishable. This thesis contributes to science by offering a framework that is drawn from recent literature, surveys and interviews, thus reflecting reality very well. It also contributes to science by offering a holistic framework applicable on a variety of organizations, covering the central parts in cyber security including, prevention, action and evaluation. Companies should use the framework as a foundation and then, if necessary, further customize aspects to fit their specific business.

6.5 Future Research

With a subject that constantly is evolving there will always be areas that can be explored in the future. Based on this thesis and the delimiters taken, there are some interesting areas to be further explored. Research can revolve around internal problems, for instance how employees purposely help cybercriminals and act out on their own. Another interesting aspect of cyber criminality is to further explore methods/programs, which enables organizations and other authorities to trace criminals and ultimately be able to hold someone accountable for the committed crimes, which unfortunately today is quite hard.

Another emerging area is the use of AI for different purposes. Further aspects to consider are how AI can be used for both anticipating incoming attacks and spot ongoing attacks. On the opposite side to this, and worth future research, is how AI can be used for criminal activity, for instance how it can be used to design malware and improve hacking abilities.

Bibliography

Alert Logic. (2018). Biggest data breached 2018 so far ***accessed from https://blog.barkly.com/biggest-data-breaches-2018-so-far***

Australian Government. Undertaking the Risk Management Processes, p. 2-11. accessed from ***https://www.finance.gov.au/sites/default/files/comcover-information-sheet-undertaking-the-risk-management-process.pdf***

Business Dictionary accessed from ***http://www.businessdictionary.com/definition /risk.html)***

CA Government. (2018). California Joint Cyber Incident Response Guide accessed from ***http://www.caloes.ca.gov/LawEnforcementSite/Documents/ California-Joint%20Cyber%20Incident%20Response%20Guide.pdf***

Chadist Patrapa. (2012). Factors Underlying Companies Response to Supply Chain Disruption: A Grounded Theory Approach, p 23.

CNN. (2017). The response to North Korea's WannaCry attack shows collective defense works accessed from ***https://edition.cnn.com/2017/12/19/opinions/wanna-cry-and-north-korea-collective-defense-opinion-krebs/index.html***

CNN Business. (2017). The hacks that left us exposed 2017 accessed from ***https://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html***

Enisa. The Risk Management Process accessed from ***https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-process***

G.A Zsidisin, S. A. Melnyk, G. L. Ragatz. (2005). An institutional theory perspective of business continuity planning for purchasing and supply management*, International Journal of Production Research*, 43(16): 3402.

Government Technology. The weakest link, 31(7) accessed from ***https://archives.erepublic.com/GT/GT_Mag_Oct_2018.pdf***

HM Government. How prepared are you. Business Continuity Management Toolkit. accessed from ***https://assets.publishing.service.gov.uk/government/uploads/ system/uploads/attachment_data/file/137994/Business_Continuity_Managment _Toolkit.pdf***

Ibrahim Al-Shourbaji, Samaher Al-Janabi. (2017). Intrusion Detection and Prevention Systems in Wireless Networks, 2(3): 1-6.

International Standard Organization (2012). ISO 22301. ISO, Geneva, Switzerland

International Standard Organization (2015). ISO 9001. ISO, Geneva, Switzerland

International Standard Organization (2018). ISO 31000. ISO, Geneva, Switzerland

Jadhav Harsh. (2018). Be Prepared: Implementing a Cybersecurity Incident Response Plan, Special Issue: 6-8. 3p.

Jawad Hussain Awan, Shahzad Memon, Sheeraz Memon, Kamran Taj Pathan, Niaz Hussain Arijo. (2017). Cyber Threats/Attacks and a Defensive Model to Mitigate Cyber Activities, 37(2):361-365.

Julie Knudson. (2018). The human errors behind data breaches, 30(2): 24-27. 4p.

Kaplan & Garrick. (1981). On The Quantitative Definition of Risk, 1(1):12-13.

Lloyd´s Register. (2018). Protecting Clients from Cyber attacks just got even better accessed from ***https://www.lr.org/en/latest-news/protecting-clients-from-cyber-attack-just-got-better/***

Manuj, I. and Mentzer, J. T. (2008). Global supply chain risk management. *Journal of Business Logistics*, 29(1):138.

M. Bartock, J. Cichonski, M. Souppaya, M. Smith, G. Witte, K. Scarfone. (2018). NIST, Special publication 800-184 Guide for Cybersecurity Event Recovery accessed from ***https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf***

MIT Technology Review. (2018). Six Cyber Threats to Really Worry About in 2018 accessed from ***https://www.technologyreview.com/s/609641/six-cyber-threats-to-really-worry-about-in-2018/***

National Cyber Security Centre. Weekly Threat Report 21st September 2018 accessed from ***https://www.ncsc.gov.uk/report/ weekly-threat-report-21st-september-2018***

PwC. (2018). Welcome to the crisis era. Are you Ready?
accessed from ***https://www.pwc.com/gx/en/ceo-agenda/pulse/crisis.html***

PwC. Är er organisation cybersäkrad?
accessed from ***https://blogg.pwc.se/foretagarbloggen/är-er-organisation-cybersäkrad?utm_source=hs_email&utm_medium=email&utm_content=70159261&_hsenc=p2ANqtz-_Ci2mYg0Ds05v__RRxk6IkXZMbdzcQ_e-l2tWA4FzyI8uJrzFtR1sst3kNR1hzumosfo36CmUatJncfU_X7ykYp8ygxg&_hsmi=70159261***

S. Sreejesh, Sanjay Mohapatra, M. R. Anusree. (2014). Business Research Methods, p. 29-32; 58.

Strategy and business. (2018). Planning for the Unexpected
accessed from ***https://www.strategy-business.com/article/Planning-for-the-Unexpected?gko=1dbff***

The guardian. (2018). British Airways hacking: Customers cancel credit cards as airline defends handling of 'sophisticated' cyber attack
accessed from ***https://www.telegraph.co.uk/news/2018/09/07/british-airways-hacking-customers-cancel-credit-cards-airline/***

Varonis. (2019). 60 Must-Know Cybersecurity Statistics for 2019
accessed from ***https://www.varonis.com/blog/cybersecurity-statistics/***

WEF, World Economic Forum (2018). Regional Risk for Doing Business 2018
accessed from **http://www3.weforum.org/docs/WEF_Regional_Risks_Doing_Business_report_2018.pdf**

A1. Interview Guide:

Part 1. Estimation of cyber risks and how to minimize effects of attacks

1. How do you work in order to estimate risks and minimize the impact of cyber attacks?

2. How do you work with business continuity management and risk management?

3. What is your view on the human error related to cyber incidents?
   How do you work with your employees in relation to cyber problems?

4. What are your routines considering software updates, who is responsible?

5. What should on think about considering back up data?

Part 2. How should one work and what is important to consider during an attack

1. What is important to consider during an attack? What is the first step?

2. Do you have an incident response/management plan and how do you operate it?

3. Do you have someone responsible on site with all responsibilities?

4. Do you have a crisis group/consultancy firm always standing by?

Part 3. The work in the aftermath of an attack

1. What is important in this stage?

2. How do you work in order to minimize future risks?

3. Do you investigate how the intrusion was possible?

4. Do you have an establish work plan?

5. What is your opinion concerning insurances?

A2. Survey Questions:

Company wishes to remain anonymous: Yes No

Type of business:

1. Have you been victimized by any form of intrusion in the last three years? Mark with a X

Yes: No: Don't know:

2. Which external threat does you consider being greatest for your business? Please describe shortly

3. How do you describe threats related to cyber attacks?

4. How do you work in order to:
4.1 Minimize and
4.2 Estimate risks related to cyber attacks?

Please describe shortly

5. During an ongoing intrusion, is there a plan on how you should
5.1 Work to limit/minimize the damage, as well as
5.2 Prevent spreading of malicious code/program

Please describe shortly

6. After a potential intrusion,
6.1 Do you update/alter your security measures, as well as
6.2 Investigate what made the intrusion

Please describe shortly

7. Do you use external expertise in the three different steps (question 4-6) If yes, within which field do you receive help?

Please describe shortly

8. How often do you update/evaluate existing security routines/security programs?

1 time/month 1 time/half year 1 time/year

9. Do you have any insurance that cover cyber related attacks/intrusions? Or insurance in the form off support if anything happens?

Please describe shortly