Jouni Aleksi Jalmari Mäkelä

Disaster Recovery Plan

Thesis

Information and communication technologies

Cybersecurity

2024

Kaakkois-Suomen ammattikorkeakoulu

Tutkintonimike	Insinööri (AMK)
Tekijä (Tekijät)	Jouni Aleksi Jalmari Mäkelä
Työn nimi	Toipumissuunnitelma
Toimeksiantaja	Kaakkois-Suomen ammattikorkeakoulu
Vuosi	2024
Sivut	51 sivua
Työn ohjaaja	Kimmo Kääriäinen

TIIVISTELMÄ

Tämän opinnäytetyön aiheena on tutkia ja luoda toipumissuunnitelma yritykselle. Toipumissuunnitelma on ohje, jonka avulla yritys palauttaa normaalit toiminnat kyberturvallisuushäiriötilanteen jälkeen. Normaali toiminta on määritelty ajankohdaksi, jolloin yrityksen eri laitteet ja toiminnot toimivat normaalisti ja ennalta odotettavalla tavalla. Toipumissuunnitelma koskee yleensä koko yritystä ja sen eri osastoja. Yritys jolle opinnäytetyötä tehdään, on pyytänyt, että toipumissuunnitelmassa keskitytään vain IT-osastoon ja sen laitteisiin. Tämä tarkoittaa myös sitä, että tämä opinnäytetyö keskittyy vain IT-osastoon.

Vaikka tämä opinnäytetyö tehdään yritykselle, yritys pysyy nimettömänä. Opinnäytetyössä tarkastellaan toipumissuunnitelmaa yleisemmin ja laaditut esimerkit, joita opinnäytetyössä on, ovat keksittyjä. Yritys saa erillisen dokumentaation, jota ei julkaista tämän opinnäytetyön kanssa. Tällä pyritään suojaamaan yrityksen tietoja ja varmistamaan, ettei tätä opinnäytetyötä voida käyttää yrityksen tietojen keräämiseen.

Tämä opinnäytetyö on tehty kehitystutkimuksena, joka seurasi monimenetelmäisyyttä tutkimus metodina. Opinnäytetyö sisältää sekä ensisijaista että toissijaista tutkimusmateriaalia. Tämä opinnäytetyö määrittelee, mitä toipumissuunnitelma on ja mitä tarvitaan onnistuneeseen toipumissuunnitelmaan. Opinnäytetyössä käydään läpi riskianalyysin hyviä käytäntöjä tutkimusmateriaalin perusteella ja lopuksi esitän yksinkertaistetun version siitä, miten riskianalyysi kuuluisi tehdä. Riskianalyysin jälkeen käsittelen toipumissuunnitelman samalla tavalla. Ensin kerron toipumissuunnitelman hyviä käytäntöjä tutkimusmateriaaliin perustuen ja tämän jälkeen esitän yksinkertaistetun version siitä, miten toipumissuunnitelma kuuluisi tehdä. Kun olen kertonut riskianalyysista ja toipumissuunnitelmasta niin kerron molempien suunnitelmien ylläpidosta.

Tämän opinnäytetyön tavoitteena oli selvittää toipumissuunnitelman teoriaa ja parantaa yritystä tarjoamalla yritykselle teoria ja pohja dokumentaatio aiheeseen liittyen. Opinnäytetyön tavoite saavutettiin. Opinnäytetyön ansiosta yritys ymmärtää paremmin, missä yrityksen heikot paikat ovat ja jos jokin menee pieleen, yrityksellä on pohja sille, miten siitä toivutaan. Muille lukijoille tämä opinnäytetyö voi olla hyvä lähtökohta, kun pohditaan toipumissuunnitelman tekemistä.

Asiasanat: toipumissuunnitelma, kyberturvallisuus, riskianalyysi

Degree	Bachelor of Engineering
Author (authors)	Jouni Aleksi Jalmari Mäkelä
Thesis title	Disaster Recovery Plan
Commissioned by	South-Eastern Finland University of Applied Sciences, XAMK
Time	2024
Pages	51 pages
Supervisor	Kimmo Kääriäinen

ABSTRACT

The topic of this thesis is to research and create a disaster recovery plan for a company. Disaster recovery plan is a set of instructions on how to return a company back to normal operations after a cybersecurity disaster has happened. Normal operations can be defined as the time when a company's assets and functions are operating in a normal and predictable way. Disaster recovery usually involves the whole company and all its different departments. The company I am making this thesis for has requested that the disaster recovery plan will only focus on the IT-department and its devices. That means that also this thesis will only focus on the IT-department.

Even that this thesis is being made for a company the company will stay anonymous. The thesis will have a more general look on disaster recovery and examples that are in the thesis will be made up. The company will receive separate documentation that will not be publicly included in this thesis. This is done to protect the company's information and ensure that this thesis cannot be used to gather information about the company.

This thesis will define what disaster recovery is and what is needed for a successful disaster recovery. I will first go over what are good rules and practices when making a risk analysis based on the research material I gathered during this thesis, after going over the good rules and practices I will present a simplified version of risk analysis. After risk analysis I will go over the same things when it comes to disaster recovery. I will go over good rules and practices and then I will go over a simplified version of disaster recovery. After risk analysis and disaster recovery I will go over how to upkeep both documentations and how to improve them. This thesis was done as a development study that followed a multimethodology as the research methodology. The thesis will have both primary and secondary research material.

The goal of this thesis was to go over the theory of disaster recovery and improve the company by providing them with theory and documentation templates related to the topic. The goal of the thesis was achieved, because of the thesis, the company better understands where the weak points of the company are and if something goes wrong, the company has a better understanding of how to recover from it. For other readers this thesis can be a good starting point when thinking about creating your own disaster recovery plan.

Keywords: disaster recovery (DR), cybersecurity, risk analysis

CONTENT

1 INTRODUCTION

The purpose of this thesis is to research how a company can recover from a cybersecurity incident that would prevent the company from doing its normal operations. Cybersecurity incident is defined as a digital or physical event that has an impact on the information technology section of the company, prompting the need for response and recovery. Normal operation is defined as the time when the company’s assets and functions are operating as expected, devices are communicating with each other, and devices that should be seen on the network are seen by the network. The thesis will be done from a theoretical point of view with some invented examples that help to explain what is being talked about.

The topic is very wide, and it has been narrowed down to only focus on defining the assets and functions of a company, doing risk analysis on these assets and functions, making a disaster recovery plan, and doing a continuity plan. Disaster recovery plan (DRP) is a plan that has the purpose of restoring normal operations in the company after an incident has happened. Continuity plan has the purpose of ensuring that after all the research and preparation is done, the DRP is followed and renewed over time, and it is not just forgotten until the incident happens. In the research material there is also talk about business continuity (BC). BC refers to all the operations that are needed so that business operations in a company can happen continuously. Disaster recovery plan is a part of BC.

As a part of this study, a DRP will be designed for a company. The company that the DRP will be made for will remain anonymous and information regarding the company will also remain a secret. The reason for this anonymity is that if the assets and the risks of the company were made public, criminals could try to use this material to find potential vulnerabilities about the company. It is in the company’s best interest that the thesis cannot be used to gather information about the company’s potential weaknesses or the company’s structure.

Cybersecurity is often viewed as digital security that has to do with networks, firewalls, and other digital assets. While this is true, it is not the full picture of cybersecurity. Cybersecurity is also physical security. If a company employee gets a malicious email and he opens it, it is also a cybersecurity incident. What about if a worker leaves their computer open when they are gone? If a malicious actor goes and uses this computer and does something malicious it is also a cybersecurity incident.

2 RESEARCH PLAN

Empirical research is based on experience with the research object. In empirical research, research results are obtained by making concrete observations about the research object and analysing and measuring it. In empirical research, concrete and collected research material is at the center of the research and serves as the starting point for doing the research. (Empiirinen tutkimus 2015.)

I chose empirical research as the research approach for this thesis because it would be very difficult to make a disaster recovery plan without making concrete observations about the research object and analysing and measuring it. Therefore, the empirical research approach was an easy choice.

In this research I am observing the current state of a company. Throughout the research I will gather information on how to develop a company. Information gathering will be done with both primary and secondary information. Primary information will be questionnaires and interviews, and secondary information will be documents and other research that has been done for this company before. Once the research has ended, the company will be developed. Based on these factors, the thesis will be a development study.

Quantitative research is a methodology in scientific research that is based on describing and interpreting an object using statistics and numbers (Määrällinen tutkimus 2018).

Qualitative research is a methodology trend in scientific research that aims to understand the quality, characteristics, and meanings of the object holistically (Laadullinen tutkimus 2018).

In scientific research, several different research methods can be used to solve the same research problem. Such a research strategy is called multimethodology. (Monimenetelmällisyys 2018).

I will be gathering information from a large group of people by using surveys. These surveys are quantitative research because I will be dealing with numbers and statistics. I will also be doing individual interviews which fall under qualitative research. Because I will be using two different research methods in this thesis, this research will be a multimethodology research.

2.1 Research layout

The objective of the thesis can be divided in to three different parts. The first part will be about examining what kind of a structure a small to medium sized company has. The second part will be what kind of risks are associated with this structure. The third part will look into if something goes wrong, how the negative effects can be dealt with effectively so that the company can return to normal operations. After the thesis is completed, the company that will receive the DRP will have a better understanding of where the risks are and how to recover in case one of these risks regarding the structure will come true.

The research problem for this thesis is the following: what is needed so that a small to medium sized company can recover from a cybersecurity incident? The research problem helps when forming the research questions. The research questions will help to guide the thesis when it is being made. Based on this research problem, the research questions are the following:

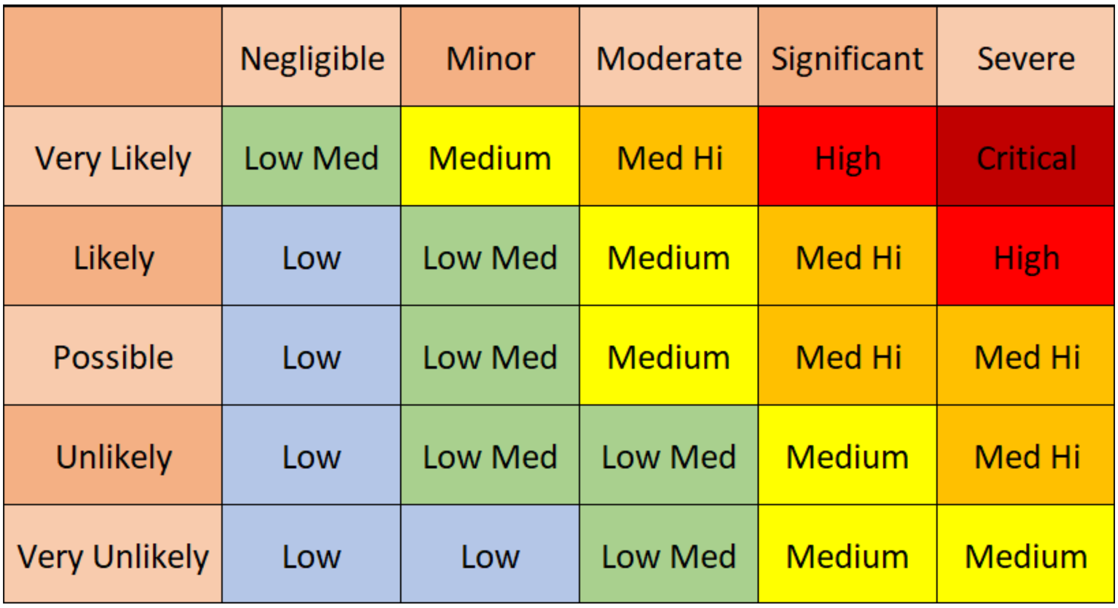
1. What are the assets and functions of a small to medium sized company?
2. What risks are associated with assets and functions in these companies?

3. How can a company recover from a loss in normal operations better?

The first question will put a focus on the correct type of company structure based on the size of the company. A large company will have a different structure than a small company, and the potential weaknesses will be different. This question will lead the research and documentation to focus on what kind of assets there are in the company. This will help the thesis stay focused and not expand into a too large of an area or focus on assets that a big company might have but a smaller one does not. The reason for why the thesis should not focus on assets that the company does not have is because the company cannot use this information for anything useful. The thesis will have an example of a small to medium sized company, and the company will have a separate document that will have specific information about their company.

The second question will help to define the risks of the structure, where the weakest parts of the structure are, and where the disaster recovery will be most likely needed. This will not only help to focus the remaining research where it is needed most, but it will also help the company allocate resources and its focus to what will most likely be the point of failure. One way this can be done is with a risk matrix that will add the likelihood of a risk happening on a scale of very unlikely to very likely, and the impact of the risk on a scale of negligible to severe.

What will be considered a negligible or severe loss to a company changes from company to company. Therefore, the thesis will have examples of risks and how they could affect small to medium sized companies, and what kind of costs these incidents would have on these companies. The company will have a separate document that will have specific information about their company.



	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	Critical
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

Figure 1. Example of a risk matrix.

The impact of the risk can be defined as how much the company will lose money recovering from an incident. For example, a negligible impact can be anything under 100 euros, minor can be something from 100 euros to 900 euros, moderate can be 1 000 euros to 9 000 euros, significant can be 10 000 euros to 100 000 euros, and severe can be everything above 100 000 euros.

The likelihood of something happening can be defined by looking at company history of incidents and looking at other small to medium sized companies and searching how often these incidents happen. As an example, very likely is something that could happen once in a month and something very unlikely can be once every 10 or 15 years.

The third question will investigate what can be done after an incident has happened, and this part of the thesis will have concrete instructions on what can be done. The thesis will have general instructions for what small and medium sized companies could do. The company that the thesis is being made for will have a separate document that will have specific information about their company.

2.2 Data extraction

According to Snedaker and Rima (2013, 168), there are numerous methods that can be used to gather data about a company's risks. They list four different methods that can be used to gather information about the risks. These four methods are the following:

1. "Questionnaires. Standardized questionnaires can elicit data from specific groups or individuals. Questionnaires can help limit input and feedback to those areas most useful."

2. "Interviews. Interviews with subject matter experts can be extremely helpful in uncovering needed information. This process is particularly helpful when you have subject matter experts who cannot or should not participate on the BC/DR team but whose input is vital. Interviews can be conducted using the questionnaire instrument to help direct and focus the interview. However, sometimes a more freeform interview can yield more information. Questionnaires often contain unintentional biases and allowing an interviewee to discuss the topic without the constraints of a questionnaire can often yield data that might otherwise have been missed."

3. "Document reviews. Reviewing corporate and organizational documents can help identify threats, threat sources, and vulnerabilities. These documents may also be extremely helpful in understanding the company's current critical processes and functions so that systems can be properly prioritized later in the process."

4. "Research. Internal and external research can be extremely helpful and often is needed to round out the data collected. Your team can gather reams of data on the frequency and likelihood of storms, earthquakes, or other natural events from a variety of governmental resources (many of which are referenced throughout this chapter). Your team can also gather data from local fire departments, police departments, and other local organizations. Finally, there may be a lot of data about past business disruptions or events archived within the company that may be helpful in understanding threats, threat sources, and vulnerabilities to things such as break-ins, thefts, utility outages, process failures, or cyber crimes to name just a few."

Another viewpoint comes from Elder J. & Elder S. (2019, 40 – 43) They do not focus on what kind of methods should be used when gathering information. Their focus is placed on what kind of information and documentation should be focused on. They talk about mission-critical functions, department evaluations, policies and procedures, regulatory codes and requirements, and useful documents.

Based on these sources it can conclude that company documentation is an important source of information. It is also important to define what the critical functions in the company are and to also put focus on company workers when gathering information.

The questionnaires will be answered by company workers that work in IT but do not work on cybersecurity. This will help to get a better idea of their cybersecurity skills and knowledge of non-cybersecurity workers in the company. The questionnaires will have 12 questions that are in the format “yes”, “no” or “I do not know”. It is important that the questions do not lead the individual answering the questions to a desired answer, because this would make the survey pointless.

Individual interviews will be conducted with workers in the company who have their work more focused on cybersecurity. Most likely the interviews will only focus on company workers but, if possible, an individual interview will also include a 3rd party service provider. Individual interviews will not have a strict format. According to Snedaker and Rima (2013, 168) this can yield more information.

Documentation research will focus on company documents. If the company has documented past incidents, this will give good information on how these incidents were fixed, as well as other important information regarding the incidents. According to Snedaker and Rima (2013, 168) documentation can also be useful in understanding the company’s critical processes.

Lastly, research in general will help to focus on internal and external threats to the company. Focusing on just interviews and company documents would leave the area of research small. By reading other research documents, books, and articles about this subject there is a better chance of finding useful information. It is important to also have focus on external threats since these can be just as disruptive as internal threats.

Both the questionnaires and individual interviews will be done at the company location, except for the individual interview that will be done with the 3rd party service provider. If there are any useful company documents to this research, I will go through them while at the company. General research does not require any specific location so it can be done on company site or somewhere else.

2.3 Data collection and analysis

It is important that the company knows what the skill level of its workers is. If there is no knowledge of the workers’ skills, there can be overconfidence or overtrust and this will lead to additional risks in the company. This is the reason why questionnaires will be a good data point for this thesis. The questions in the questionnaires can be found in Appendix 1.

The individual interviews will give important information about the individuals’ cybersecurity skills. The individual interviews will be done in a free format in which I will be asking questions about the company and the person being interviewed will answer these questions freely. This is done because according to Snedaker and Rima (2013, 168), sometimes a more freeform interview can yield more information.

In this research I had the opportunity to interview four people. Because the identity of these people is not vital information for the research, I will give only a short description of what their responsibilities and titles are. The first person, who will be referred to as person 1 or P1 for short, is an IT manager. The second person, who will be referred to as P2, is a factory manager. The third person, who will be referred to as P3, is a cloud architect. The fourth person, who will be referred to as P4, is a factory manager. I have divided the individual interviews into four different themes. Each different theme has its own questions. The themes and questions can be found in Appendix 2.

The individual interviews are done with the idea that they help the company that the DRP in made for. Because the interviews yielded mostly information that is company specific, I will not be making any references from these interviews into the public thesis. The interviews will be instead used for making private documentation for the company.

2.4 Objective

The objective of the thesis is to research how to do risk assessment and disaster recovery on a theoretical level. After this I will make simplified versions of both the risk assessment and disaster recovery based on the research that was done during this thesis. These simplified versions are done from a general point of view, and they can be used as a base when making a risk assessment plan or a disaster recovery plan. Because risk assessment and disaster recovery need constant updating, I will also do a continuation plan that will have instructions on how to practice and upkeep risk assessment and disaster recovery documentation.

On top of this theoretical work, a goal of this research is to provide a company with theoretical knowledge on risk assessment, disaster recovery and how to upkeep this documentation. Also, to do research on the company and help the company in this way. The company will be provided with basic templates that will help the company develop their disaster recovery plan.

3 THEORETICAL FRAMEWORK

3.1 Existing research material

I have selected two books that I will read and research for this thesis. Even though the books are a reliable source of information, and they are good for research, it is still good to cross reference them and not just trust one book on all the information. Cross referencing two books from different writers is a good way to get accurate information.

The first book is called Business Continuity and Disaster Recovery Planning for IT Professionals. The book has been written by Susan Snedaker and Chris Rima. The book is from 2013. Because the book is 10 years old, there is information that is outdated, but I have chosen this book because it can still give valuable information about key concepts of disaster recovery.

The second book I chose is called Faster Disaster Recovery The Business Owner’s Guide to Developing a Business Continuity Plan. The book has been written by Jennifer H. Elder and Samuel F. Elder. The book is from 2019, so the information on statistics is much closer to what it is today. By comparing these two books together I should get a good overview on what it takes to make a successful disaster recovery plan for a company.

3.2 Risk analysis

According to Snedaker and Rima (2013, 113) risk assessment is defined as the phase in which all potential risks to the business are listed and then evaluated both for likelihood of occurrence and impact in the event of an occurrence. They also talk about defining a cut-off point for risk that should not be addressed. This is done to help manage the project.

No matter if we are talking about a small, a medium or a large company, it will have risks that can disrupt the normal operations of the company. The first thing that needs to be done in a disaster recovery plan is to map out the assets of the company and then map out the risks that affect these assets. Risk analysis is not only important for this thesis, but it is necessary for the creation of a disaster recovery plan.

STRIDE is an acronym that focuses on finding threats by looking at different actions, these actions are spoofing, tampering, repudiation, information disclosure denial of service and elevation of Privileges. In short spoofing means impersonation someone else, tampering means modifying code or documents, repudiation means claiming to not have done an action that was actually done, information disclosure means exposing information to someone that is not authorized to see it, denial of service is denying access to services by other users, and elevation of privileges is getting higher authority without proper authorization.

Persona non Grata (PnG) is a method where the focus is put on trying to imagen the attacker, his or her motives, and skills. PnG forces thinking outside the box and thinking from an unconventional viewpoint. PnG does not focus on assets and functions directly and using this method can leave a lot outside the analysis.

Using ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment. (ISO 31000, 2018)

ISO 31000 is a standard for risk management. There are few reasons for why I will not be using ISO 31000 in my thesis. Reason one is that this thesis will only go over risk analysis and will not cover risk management, and using a standard for risk management would not provide that much research material for this thesis. Reason number two is that even if this thesis would use ISO 31000 this thesis could not be used to validate this standard because this thesis would not cover ISO 31000 as a whole. For these reasons I have decided not to use ISO 31000 when doing research for this thesis.

I previously mentioned that I will use a risk matrix in this thesis. There are a few reasons for why I have chosen a risk matrix as the way I want to present the risks of this research. The first reason is that I wanted to use something that is visual rather than just having a document that has a lot of text. When there is something visual to show it makes it much easier to understand the risks and their severity. The second reason as to why I have chosen a risk matrix rather than for example a risk tree, is because a risk tree can get large, making it hard to present, read and understand.

3.3 Disaster Recovery

“A disaster recovery plan is essential in keeping an organisation’s data accessible and protected.” (Townsend 2022). A disaster recovery plan is something that is usually associated with large companies that have a lot of resources available to them, but disasters can happen to a company of any size. Therefore, disaster recovery should be a concern no matter the size of the company.

No matter how much time, focus and effort are put on security and making sure everything works, over time eventually something will go wrong. When something goes wrong, there needs to be a plan on how this incident will be eliminated and how the system will be restored to normal. It is important that the plan is clear and that there are multiple people who know how to execute the plan effectively. The reason why multiple people are trained for every step is to make sure that one single person does not become a single point of failure in the plan.

3.4 Continuation plan

After we have spent all this time and resources mapping out risks and we have made recovery plan, it is important that we do not stop there. Starting from risk analysis, the company will keep changing when time goes on and this means that there will be new risks that need to be taken into consideration. Doing regular risk analysis in the company will help the company stay on top of the risks and make it less likely that something unexpected happens, that the company is not prepared for.

When the company keeps changing and new risks are found, these new risks cannot just be ignored. It might be the case that a new risk can seem small and insignificant but if it is left out of documentation, it might grow or it might affect other risks in the future. In the future, the company maybe does not find this risk again and because of it they do a miss evaluation on another risk that leads to a big problem. When new risks that affect the company are discovered, the recovery plan needs to be updated.

Good documentation is important to having a successful recovery but what if this documentation is not used and practiced? When we are put in a high stress situation, we make mistakes, and we need more time to think. The faster we can recover from a disaster the better it is for the company. Therefore, it is important to do training and practice different scenarios.

4 RISK ANALYSIS

In this section I will explain the reason why a risk analysis is important when making a disaster recovery plan. I will first go over the information that is connected to assets and functions. Second, I will go through risks and their costs to a company. Lastly, I will talk about good rules about documentation. The thesis will have a more general view on what is good to know when doing a risk analysis and what assets to consider while making a risk analysis. The company will have separate documentation that is tailored to them.

4.1 Risk analysis methods

A good place to start is to think about different methods for gathering information. Snedaker and Rima (2013, 168) talk about the methods for gathering information. These methods are questionnaires, interviews, documents, and research. Since these methods were already covered and explained in section 2.2 of this thesis, I will not go over them again.

Snedaker and Rima (2013, 203) talk about the difference between quantitative and qualitative threat assessment, and they give an example. A quantitative assessment involves measurements and numbers, they are specific and measurable. Saying that, “The server costs $1850 more than the desktop system,” is making a quantitative statement. In contrast, if you say, “The server is more expensive than the desktop system,” you are making a qualitative assessment, because “more” is not specific or measurable.

Elder, J. & Elder, S. (2019, 67 – 68) give three risk assessment methods to consider. These include employee surveys, PESTLE analysis, and SWOT analysis. The employee survey method is a method where you ask your employees about their opinions of risks. They state that since the employees are the most familiar with the day-to-day operations of the organization, they also know where the weaknesses are. PESTLE analysis stands for political, economic, social, technological, legal, and environmental analysis. This type of analysis is an effective tool for brainstorming the external environment in which your company operates.

After PESTLE Elder, J. & Elder, S. (2019, 69) explain SWOT analysis. They describe SWOT analysis as a brainstorming tool that helps to better identify the positive and negative effects of both internal and external factors. SWOT stands for strengths, weaknesses, opportunities, and threats. They state that, it is important to understand that strengths and weaknesses are internal. Opportunities and threats are external.

Elder, J. & Elder, S. (2019, 54) talk about identifying and evaluating risks. They mention that a common mistake many companies make is seeing this as a one-and-done event. They continue by stating that the world is a risky place and getting riskier all the time. I have interpreted this as them saying that identifying and evaluating risks is a process that needs to be constantly done.

4.2 What to include in a risk analysis

Elder, J. & Elder, S. (2019, 2 – 3) talk about disaster timing and size. They bring to light the idea that even small disasters like a computer virus, water main break, the loss of a supplier or negative press can have huge effect on the company. They also bring to light how different sizes of companies effect the impact of the disaster.

Snedaker and Rima (2013, 27) talk about the types of disasters to consider. They divide disasters into three categories. These categories are natural, human-caused, and accidental/technical. Natural disasters can be caused by hot and cold climates, and other examples can be earthquakes, tsunamis, volcanic eruption, or land shifting. Human-caused disasters can be in the form of terrorism, cyber-attacks, or protests, to name a few. Accidental/technical disasters can be transportation accidents, infrastructure failures and hazardous materials accidents.

Elder, J. & Elder, S. (2019, 3) also talk about the different disaster types. They list environmental, biological, deliberate, utilities, equipment, information technology and other as the different categories. All authors list and talk about the same disaster types, but they use different specific names. Combination of both these sources will give a good list of disaster types to consider when making the risk analysis.

Snedaker and Rima (2013, 133) talk about network vulnerability assessment. To maintain a low security threat profile, it is important to have information about how assets are seen on the network by unauthorized users and how they respond to network requests on the open physical and logical ports. It is important that an organization scans the network and produces actionable reports for all levels of network vulnerabilities. Snedaker and Rima also state that it is good to have outside audit firms performing these scans. Also, when changes are made, it is important to update the vulnerability assessment.

Snedaker and Rima (2013, 166) talk about risk assessment components. They say that the risk assessment process is shown in the shaded area in Figure 2. They state that there are three distinct steps defined in the preceding section. In Figure 2 these three distinct steps seem to be Threat assessment, Vulnerability assessment and Impact assessment. Figure 2 is derived from Figure 4.2 shown in Snedaker's and Rima's book. I have made a new version of the figure to make the risk assessment process clearer and easier to understand.

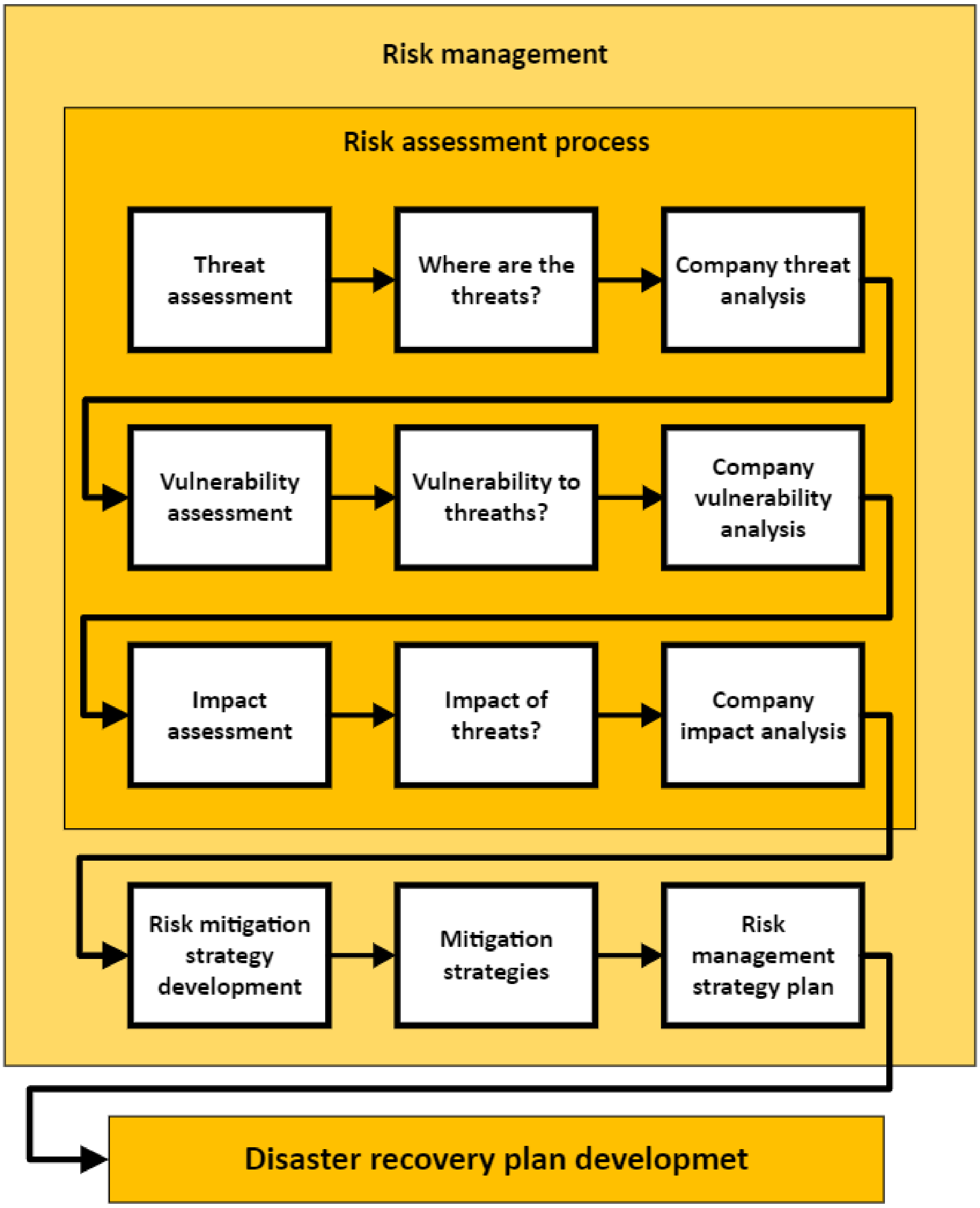


Figure 2. Risk assessment process based on Figure 4.2, Snedaker and Rima (2013, 154).

Threat checklist is a list of threats that should be done when doing threat assessment. Threat checklist should cover a wide base of different threats, meaning that even stuff that might not sound like a threat at first should be listed. Snedaker and Rima (2013, 199) give an example of a threat checklist and say that it can be used as a starting point in a threat assessment.

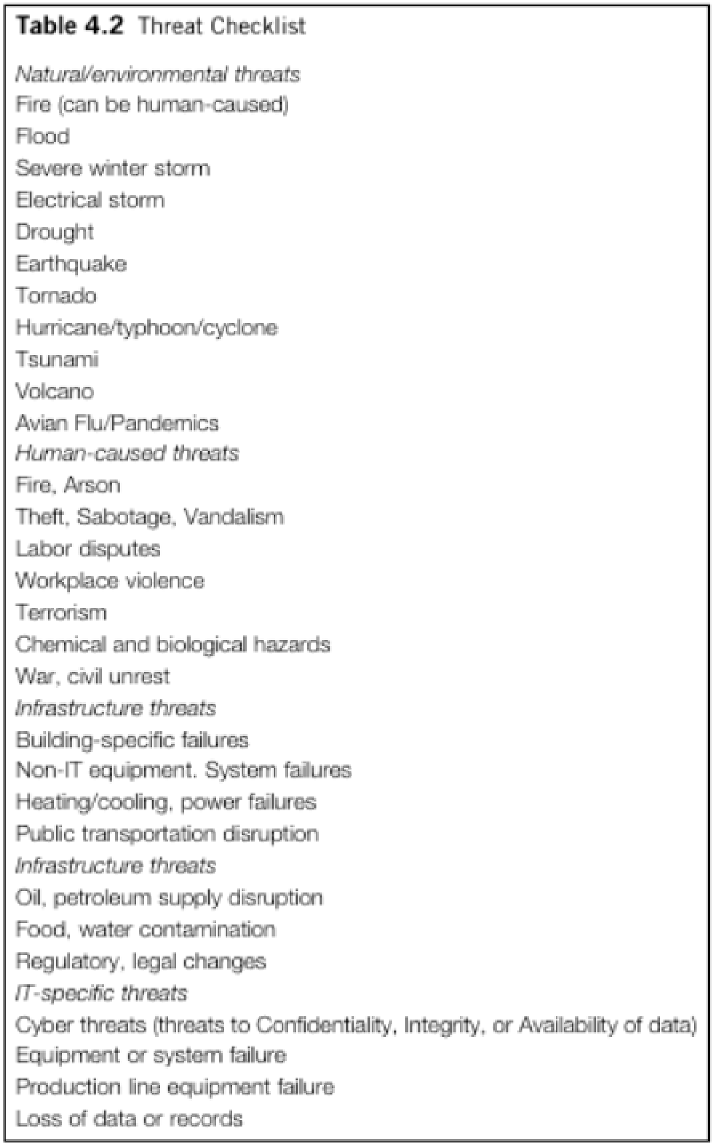


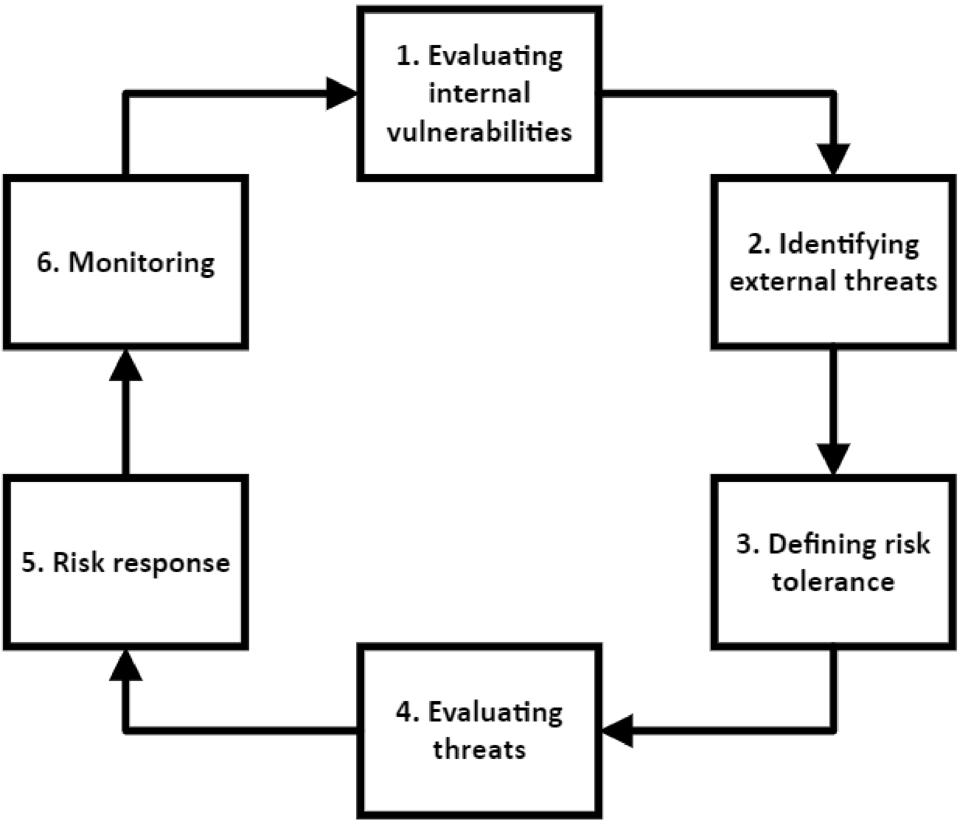
Table 4.2 Threat Checklist

Natural/environmental threats
Fire (can be human-caused)
Flood
Severe winter storm
Electrical storm
Drought
Earthquake
Tornado
Hurricane/typhoon/cyclone
Tsunami
Volcano
Avian Flu/Pandemics
Human-caused threats
Fire, Arson
Theft, Sabotage, Vandalism
Labor disputes
Workplace violence
Terrorism
Chemical and biological hazards
War, civil unrest
Infrastructure threats
Building-specific failures
Non-IT equipment. System failures
Heating/cooling, power failures
Public transportation disruption
Infrastructure threats
Oil, petroleum supply disruption
Food, water contamination
Regulatory, legal changes
IT-specific threats
Cyber threats (threats to Confidentiality, Integrity, or Availability of data)
Equipment or system failure
Production line equipment failure
Loss of data or records

Picture 1. Picture of Table 4.2 Threat checklist, Snedaker and Rima (2013, 200).

Elder, J. & Elder, S. (2019, 54) talk about the risk assessment process. They define risk assessment as a process designed to identify and evaluate threats and hazards that could potentially harm the company. Risk assessment involves considering different types of threats that exist, assets that are at risk from these threats, and the potential negative impacts of these threats. They also state that company’s assets come in many different shapes and forms, and that risk assessment should consider the impact on all of them. The assets include people, data, equipment, facilities, proprietary information, utility systems, raw materials, supplies, inventory, and reputation.

Elder, J. & Elder, S. (2019, 54) continue, people’s safety should be the most important thing to consider. These people include employees, vendors, customers, and other people that are involved in the business. Response plans should be created to handle any threats that could cause personal injury to them. Another thing that they say should be done when making a risk assessment is to look at vulnerabilities. They tell to think about where are the weakest links that could create the most damage and how to address each one of these weaknesses. On page 55 there is a Figure 8.1. The figure describes risk assessment process from in their opinion. The risk assessment process is show in a circle diagram. Picture 3 is derived from Figure 8.1 to make the risk assessment process clearer and easier to understand.


1. Evaluating internal vulnerabilities
2. Identifying external threats
3. Defining risk tolerance
4. Evaluating threats
5. Risk response
6. Monitoring

Picture 2. Risk assessment process based on Figure 8.1, Elder, J. & Elder, S. (2019, 55).

Elder, J. & Elder, S. (2019, 55 – 67) state that accepting the risk and doing nothing is an option that can be done. They also give another alternative that is to avoid the risk entirely and take steps to mitigate damages. After this they explain each of these steps that are shown in picture 3.

Step 1: In this phase, the company develops a thorough understanding of their business processes and where they might break. This is done by collecting information about the organization in its current state. This includes the specific operations of each department and the functions necessary for normal operations. This step includes listing physical locations, looking at the area outside of the facility, understanding materials that are stored, locating shut-off valves, panels, and fire extinguishers.

Step 2: In this step you should try to identify as many external threats as possible. In this stage quantity is more important than quality. They explain that there are eight external threat areas to consider. These eight areas are environmental, biological, deliberate disruption, utilities, equipment, information technology, economic and other.

Step 3: In order to know how you can address various types of risks you need to know what the risk tolerance for you company is. Risks are defined in terms of loss, which may include downtime costs, impact on customers and violation of regulations. Questions that should be asked when in this step are how much money can your organization afford to lose? How much server downtime is acceptable? How long can you go without access to your data? How long would it take for your customers to be affected if you telephone lines or website go down? Are there any regulations that specify your maximum downtime?

Step 4: Since it would be impossible to address all potential threats there needs to be prioritization to determine which threats will be addressed first. This can be done by estimating the likelihood of occurrence, the potential extent of human, physical, and business impact, resources available to address the threats, and the amount of time it will take to return to normal operations.

Step 5: In this step they suggest reviewing top five threats and look for consistencies and similarities between them. Also, they suggest looking for similarities regarding resources. They state that a part of risk analysis is determining how your organization wants to address each threat. There needs to be a decision does the company want to accept the threat, avoid it entirely, or take steps to mitigate the impact. This mitigation may involve insurance, taking steps to prevent or reduce the impact. Since each company will have its own tolerance to risks, each company will have to make a plan that fits them.

Step 6: The last step in the process is to monitor the situation. Updating the analysis should be done at a minimum, once a year. The company needs to monitor itself, customers, vendors, and external environment for changes that could create new risks or change the ranking of an existing threat.

Last thing that Elder, J. & Elder, S. (2019, 72.) talk about in this chapter is assigning a chief risk officer. They say that every project needs a leader, that is assigned the responsibility for getting the project done and making sure it gets updated. That is why it is important to have a designated chief risk officer, or CRO. CRO will also be tasked with coordinating safety training, developing risk action plans, leading the business continuity planning team and leading the emergency response team.

4.3 Threat assessment

Snedaker and Rima (2013, 166) begin by discussing threats and threat sources. They put emphasis on the difference between these two. An example they give of a threat would be power outage. An example of a threat source could be a failure in the power lines, a failure in the transformer, or a failure in the whole power grid. They state that in general discussion of threats it often not very useful to discuss a threat source separate from the threat. However, thinking about threats and threat sources as separate things can help to discover potential risks that were previously unknown.

Snedaker and Rima (2013, 169 – 184) talk about natural and environmental threats. They mention fire, floods, severe winter storms, electrical storms, drought, earthquake, tornados, tsunamis, volcanoes, and pandemics. After mentioning these threats, they explain how they might affect the company’s ability to function.

Snedaker and Rima (2013, 185 – 194) talk about human threats. They mention fire, theft, sabotage, vandalism, labour disputes, workplace violence, terrorism, war, and cyber threats. They explain these threats and how they might affect the company’s ability to function.

Snedaker and Rima (2013, 195 – 198) talk about infrastructure threats. They mention building-specific failures, public transportation disruption, loss of utilities, petroleum shortage, food, or water contamination and regulatory or legal changes. They explain these threats and how they might affect the company’s ability to function.

4.4 Vulnerability assessment

Snedaker and Rima (2013, 211) define vulnerability as various areas of the business that are exposed to threats defined in the risk assessment phase. They give examples of how the likelihood of a threat event occurring can be defined. The table has three sections. One with qualitative value, going from very high to very low, second with semiqualitative value, going from 100 to 0, and third where there is a description of what each of these values holds in.

After the first table there is a second table that gives an example of how the likelihood of adverse impact can be defined. The table has three sections. One with qualitative value, going from very high to very low, second with semiqualitative value, going from 100 to 0, and third where there is a description of what each of these values holds in.

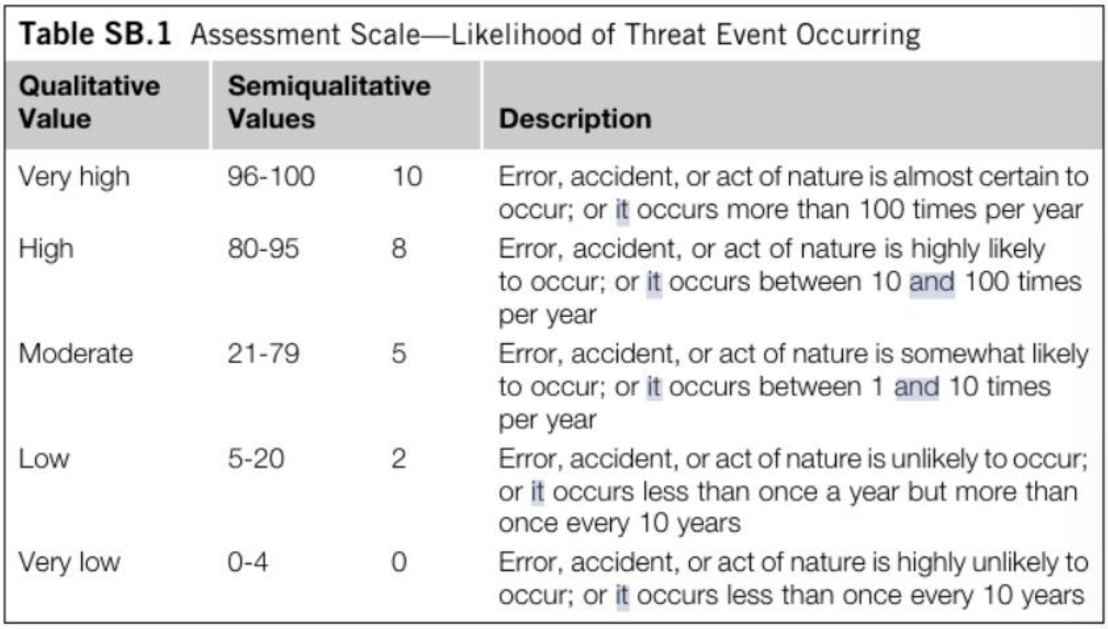


Table SB.1 Assessment Scale—Likelihood of Threat Event Occurring

Qualitative Value	Semiqualitative Values		Description
Very high	96-100	10	Error, accident, or act of nature is almost certain to occur; or it occurs more than 100 times per year
High	80-95	8	Error, accident, or act of nature is highly likely to occur; or it occurs between 10 and 100 times per year
Moderate	21-79	5	Error, accident, or act of nature is somewhat likely to occur; or it occurs between 1 and 10 times per year
Low	5-20	2	Error, accident, or act of nature is unlikely to occur; or it occurs less than once a year but more than once every 10 years
Very low	0-4	0	Error, accident, or act of nature is highly unlikely to occur; or it occurs less than once every 10 years

Picture 3. Picture of Table SB.1 from the 2013 book on the likelihood of a threat event occurring, Snedaker and Rima (2013, 212).

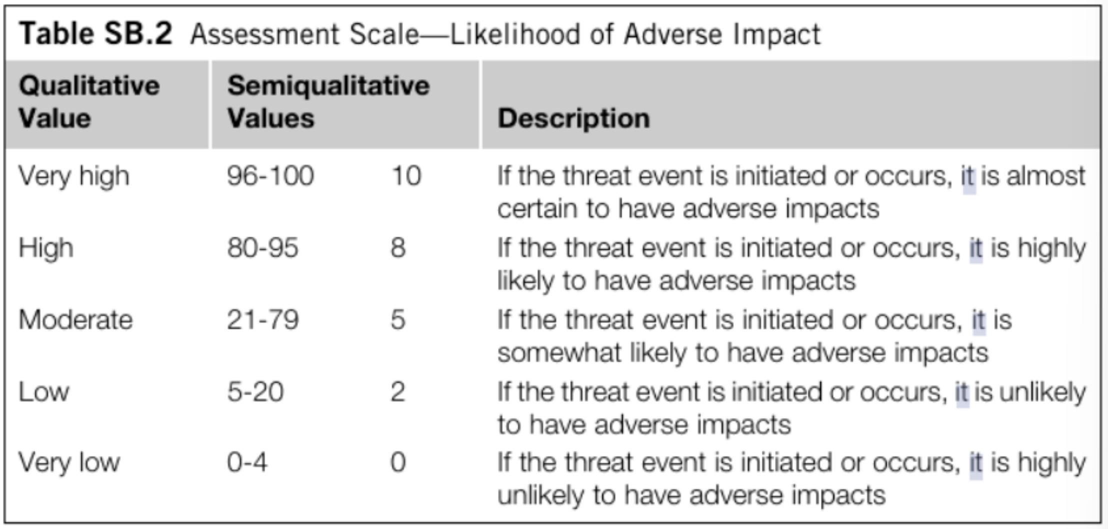


Table SB.2 Assessment Scale—Likelihood of Adverse Impact

Qualitative Value	Semiqualitative Values		Description
Very high	96-100	10	If the threat event is initiated or occurs, it is almost certain to have adverse impacts
High	80-95	8	If the threat event is initiated or occurs, it is highly likely to have adverse impacts
Moderate	21-79	5	If the threat event is initiated or occurs, it is somewhat likely to have adverse impacts
Low	5-20	2	If the threat event is initiated or occurs, it is unlikely to have adverse impacts
Very low	0-4	0	If the threat event is initiated or occurs, it is highly unlikely to have adverse impacts

Picture 4. Picture of Table SB.2 on the likelihood of adverse impact. Snedaker and Rima (2013, 212).

Snedaker and Rima (2013, 213 – 216) state that the BC/DR plan must include IT systems, but it should not be limited to IT systems. They state that the focus should be put in a wider area so that the BC/DR plan is complete. After this they talk about the vulnerability of people, process, technology, and infrastructure.

People: They want you to think about how vulnerable are your staff are to the threats that have been identified? Some threats may only impact people at their work, but other threats maybe not only impact the staff when they are working but also impact them outside of work. Snedaker and Rima state that people are vulnerable to phishing and social engineering. They also state that there is no system that can stop a person from giving their account to an attacker.

Process: It is a good idea to think about how vulnerable your company's processes are to different threats. The company might have processes in place that already give protection against threats. For example, the company might already have a process in place that handles short power outages. This is why it is good to think about other processes that the company might already have in place. Other processes might be completely without any sort of protection against threats.

Technology: Technology is vulnerable to many different threat sources and people who are IT professionals are aware of the most common ones. A company might have already thought about the vulnerabilities of its servers and websites when it comes to internal threats. In this risk assessment process, there also needs to be focus on external threat sources such as different natural disasters. There should not be assumptions that the current emergency plan covers all of the threat sources that could affect different systems. This topic should be approach with fresh eyes to see what else you can add to the process.

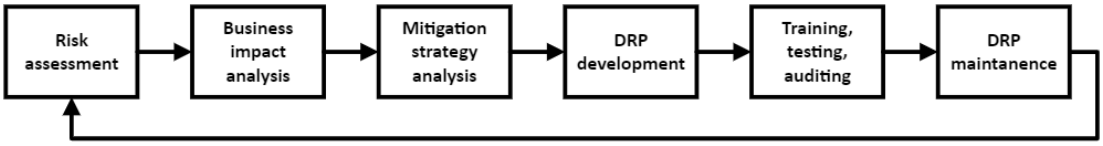
Infrastructure: When looking at the infrastructure it is important to be mindful of the geographical location. Some places might be more vulnerable to floods or heavy rain, other places might have more extreme cold or hot temperatures. It is also good to look at the inside infrastructure. A broken pipe that causes water damage to the servers is just as impactful as flooding.

4.5 Impact assessment

Elder, J. & Elder, S. (2019, 65) suggest that impact evaluation would be done in a way that you take the dollar amount that the incident would cost and then you multiply it with the probability of it happening. The events that have the cost after the probability has been counted in should be considered first.

Snedaker and Rima (2013, 22) tell that once risks have been defined the attention needs to be turned to the potential impacts that these risks can have. They put emphasis on thinking how the business will be impacted if one of these risks happen. They ask you to think about can these impacts be tolerated. They give an example where Electronic Medical Record application cannot be down, but Web servers and reporting tools can. They describe both events as disruptive but the other cannot happen while the other can.

Snedaker and Rima (2013,113) state that business impact analysis looks at how the business would be impacted if the risks were to occur. They place this step after the risk assessment so that only the risks that are important are addressed. They show figure 3.6 which shows business continuity and disaster recovery project plan progress.



Picture 5. Flow chart of the DRP based on Figure 3.6 by Snedaker and Rima (2013, 114).

Snedaker and Rima (2013, 232) talk about how critical functions are to the business. They divide criticality into 4 different sections, critical functions – mission-critical, essential functions – vital, necessary functions – important, and desirable functions – minor.

Snedaker and Rima (2013, 233) define mission-critical business processes and functions as those that have the greatest impact on the company’s operations and the greatest need for recovery. The processes that have to be present for your company to work are mission-critical. From an IT perspective these functions would be network, system or power delivery related.

Snedaker and Rima (2013, 233 – 234.) state that some business functions that fall somewhere between mission-critical and important may be labelled essential or vital. If the company cannot make the distinction between mission-critical and vital, then this category is not needed. This category should not be forced into the system and if it is not, then there will just be three categories which are mission-critical, important, and minor.

Next Snedaker and Rima (2013, 234.) talk about important business functions and processes. In a short timespan these will not stop the business from operating, but in the longer run they will have an impact if they are not resolved. When important business functions are missing, it will cause some disruption to the business. From an IT perspective, these functions may be e-mail, internet access and other tools that are used in support or reporting function.

Lastly Snedaker and Rima (2013, 234.) talk about minor business processes. Minor processes are often developed to deal with small issues, that are recurring. These functions are not needed in the near-term and they certainly will not be the main focus when the business is going through a recovery. When thinking about the long-term minor processes should be recovered. During significant disruptions some minor business processes may be lost and in sometimes it will not be a big deal.

Snedaker and Rima (2013, 235 – 238) talk about recovery time requirements. The book introduces the idea of maximum tolerable downtime (MTD). This is defined as the maximum time a business can tolerate the absence or unavailability of a particular function. This consists of two elements, the system recovery time, and the work recovery time. System recovery time is defined as the time that it takes to have the system back. Work recovery time is defined as the time it takes to have the system in normal operations again. Total recovery time on a mission-critical asset is 0-12 hours, vital asset is 13-24 hours, important asset is 1-3 days and minor asset is more than 3 days.

4.6 Simplified risk analysis

Based on the previous information this chapter will simplify the risk analysis process. To simplify the risk analysis process, I would divide it in to four different stages. First stage being the initial assessment, where all the possibilities are looked at. Second stage is vulnerability assessment, where the threats are looked and those that are not relevant are removed. Third stage is impact assessment, where company looks at the threats and figures out how much would it cost if this threat would happen to this company. Fourth stage is Risk mitigation, where risks that can be mitigated are mitigated, the situation is monitored, and the documentation is reviewed and refined.

The first step is to do an initial assessment of the situation. During this step the company will gather information about its assets, functions, and potential threats. It does not matter what format is being used during this step, but the threats that should at least be looked at are natural, human caused, technical, utility, equipment, and network threats. From this step the company should be left with a list of all the assets and functions and a threat checklist.

When making this list it is not important to think about the threats any further, in this step the only thing that matters is that every single threat is listed. When making this list it is good to have people from different backgrounds and fields making this list. A person that has been working in logistics their entire life has completely different mindset than a person that is working in IT. Both people know about the critical areas of the company, and both can contribute to the initial assessment.

While getting different departments of the company involved it is also a good idea to have different levels on those departments take part. In other words, it is good to involve people from all different positions of the company. While a manager has a deep understanding of the operations and can list threats and threat sources better than anyone else, a manager might miss something that an employee might think of, because they face different challenges every day.

When looking at the network of the company it is beneficial to use existing templates when thinking of threats. One example of an existing model is

STRIDE. As covered earlier STRIDE is an acronym that means. When thinking about these threats and trying to find how they could happen in your network should have a safer network than if you did not look at these possibilities.

While the network is important, when doing a risk analysis, the whole company needs to be considered. This does not only mean the networking side of all the different departments but also the physical side of them. If the network goes down work cannot be done, if there is a fire or other incident that affect the physical safety at the company work also cannot be done. There is also the human element that needs to be considered. What are the places where workers could face accidents that lead to incidents.

After this extensive list has been made and all the threat sources and threats have been listed, it is time to look into how vulnerable the company is to those threats. This is done by looking at how likely it is that this threat ends up happening and how likely it is that because of this the company’s asset would go out of normal operations. During this step the company will also decide what are the tolerances for different assets and functions, this will result in a list that has mission critical, important, and desirable functions. During this step all the threats and threat sources that are simply impossible are listed out. After this step the company will have a new list where only the threats that are important are listed.

An example of this would be to look at natural disasters. Is it possible that there is a hurricane that would put our asset out of use? What about extreme temperature, like heat wave or extreme cold? How about extreme flooding? Then the company will decide is the threat possible or not. The company can decide that there is no way that at our location we will have a hurricane that will put our asset out of normal operations. Yes, it might be possible that our asset might be vulnerable to extreme floods. This is done for all the assets and functions that the company has.

Now that only the threats that are relevant are left its time to do impact assessment, during impact assessment we combine the likely hood of the risk happening and the cost it will have on the company. Doing an impact analysis is very difficult and getting an accurate estimate for the cost and the probability is more than difficult. How much will this cost for the company? First there is the initial cost to recover the broken asset, then there is the cost of the lost operations. Every moment the asset is not doing its normal operations it is losing money for the company. Then there is reputation, and the question becomes how much is a good reputation worth? This is also very difficult, but a good idea would be to look at the situation and ask would this bother me as a customer and how likely is it that this customer will not want our services again?

If a customer has time sensitive orders from a company and the company fails to deliver on these orders in the promised time frame, first issues might come with the contract, maybe it is already written in the contract how much compensation the customer will receive in case the order cannot be done in the promised time frame. Second question comes down to is this customer going to order from us again? Here really good communication skills are important. Being able to communicate to the customer what has happened, how it is being fixed and how long will it take to fix is a good place to start. Also, when thinking about reputation it is good to think how other people that are not yet our customer but are considering it see this situation. Again, communication is key.

It is difficult to put a price on this, but a good way to look at it is to think if I was the customer would I trust this company again? If I was the customer how long would I wait in case of a disaster. If I was the customer, what would I like to know and what would I like to hear that would convince me to keep working with this company.

Impact assessment should be done by using quantitative statements, “Asset X will break on average every 5 years, and it will cost the company 10 000 euros, because this asset and these operations will be out of use for a week which will cost the company 9 500 euros and a new X will cost 500 euros. To mitigate this risk, we would need to re design a large portion of our infrastructure and this would cost an estimated 50 000 euros. Return of investment would be in 25 years, because of this the mitigation will not be done. In this case we will make a disaster recovery plan for this asset so we can return to normal operations as soon as possible after the asset breaks.”

After we have done the impact analysis, we can compare the cost of the threats and compare them to the cost of fixing the threat. We are left with two options, situations where the cost of mitigation is lower than the cost of the impact and situations where the cost of mitigation is higher than the cost of the impact. From this the company will have two lists, a list of assets where the threats can be mitigated and a list where mitigation cannot be done.

It is important to look at multiple assets in the same area and look at the combine cost of mitigation and impact. If multiple assets can be more secure with a single mitigation it might be more cost effective and therefor mitigation can be done. There is also a possibility that even when direct mitigation cannot be done there are other things that can be done to extend the life of an asset.

The last thing to do is to monitor the situation and see how it develops. When there are changes in the system or some new information comes about, it is important to review and refine the existing documentation. If the review and refinement is not done, it will be forgotten and there will be more problems in the system. It is important to update the documentation whenever there are changes.

At some point the company has mitigated all the threats that it can. Despite this there are still assets that are vulnerable to threats, but the mitigation cannot be done. This is where we get to the main part, which is to plan for these situations where the company has concluded that best way to treat the threat is to accept it. The best thing is to make a plan that allows the company to return to normal operations as fast as possible after the incident.

5 DISASTER RECOVERY

5.1 Preparing for a disaster

According to Elder, J. & Elder, S. (2019, 76 – 78) the first stage of disaster recovery is prevention. During the prevention stage the company will do what it can to minimise the chance that a disaster happens. They say that the company needs to think about what actions need to be taken so that injury, damage, or harm can be prevented from happening.

Before a company has an accident, it would be good to define when the company activates its disaster recovery plan and in what extent does the company activate it. Snedaker and Rima (2013, 376) suggest a use of three-level rating system. This rating systems is divided into minor disasters, intermediate disasters, and major disasters.

Snedaker and Rima (2013, 376 — 377) define a minor disaster as those where the effects are isolated to one component, one system, one business function, or just one segment of a critical business function. Normal operations can often continue. Critical business functions can still function for some time. Minor disasters can usually be resolved while the rest of the business functions normally.

Snedaker and Rima (2013, 377) define intermediate disaster as a type of disruption or disaster that interrupts or impacts one or more mission critical functions, but not all of them. Normal operations will experience significant disruptions. Entire systems or multiple systems may be unavailable, but some will still be functional. This type of event could be a fire or flood in the building that impacts IT systems and equipment.

Snedaker and Rima (2013, 378) define major disaster as an event that disrupts all or most of the normal business operations and all or most of the critical business processes. The disruptions occur because all or a majority of systems and equipment have failed or are inaccessible. A major disaster could be the destruction of the entire network, subnets, or sections of the business.

5.2 Actions and communication

According to Elder, J. & Elder, S. (2019, 78 – 81) the second stage is incident response. Incident response is the stage where the company will prevent further damages and start fixing the situation. They say that when a disaster happens it is good to have a clear chain of authority with one person in charge. This person will be responsible for implementing the response plan, overseeing the emergency response, doing situational analysis and provides crisis communications.

According to Elder, J. & Elder, S. (2019, 81 – 82) the third stage is business continuation. Business continuation is the stage when the crisis has been stopped but there are still steps left before the company can return to normal operations. When preparing for this stage of the plan the company should consider how will it get the necessary supplies, what the employees will do, and how will the business functions be restored.

Snedaker and Rima (2013, 375 — 376) activation phase is the phase during and immediately after the disruption. This is the phase where you decide what parts of your plan will be activated and in what manner. They tell to not activate your plan for every little glitch your business runs into. Activation includes initial response and notification, problem assessment and escalation, disaster declaration, and plan implementation. After you have begun implementing your plan you proceed into recovery phase.

Snedaker and Rima (2013, 381) explain that recovery phase comes after the immediate aftermath of the disruption or disaster. Usually during this phase, it is assumed that the cause of the disruption has been stopped or contained. This phase might include evacuating the building, removing equipment that can still be saved, assessing the situation, and determining which recovery steps are needed so that operations can return to normal.

According to Snedaker and Rima (2013, 382) business continuity phase kicks in after the recovery phase and defines the steps needed to get back to normal operations. Where recovery phase is about salvaging equipment, ordering new parts, and loading up backup data, business continuity phase is about having all the pieces and knowing how to put them together so normal operations can be resumed.

Snedaker and Rima (2013, 400) talk about communications plans. They state that a communications plan should have names of the people that do the communications, their responsibilities, their boundaries, a description of when they should do these communications, and other important information. They also state that communications plans can be assigned to existing teams and that there is no need to create additional teams just to execute communications plans if these activities fall within the scope of already existing teams. It is also possible that making a specific team for communications make sense, for instance to ensure that there is control over communications.

Snedaker and Rima (2013, 400 — 401) talk about internal communications. Internal communication is communication to people that are responsible for disaster recovery and people that are employees at the location. Communication between those that are responsible for disaster recovery is critical. How will team members be notified, how will they receive updates, and what processes are needed, are important things that should be considered. Employees should also be notified, and the basics of the situation should be explained to them. Employees should know what happened, what is being done to address the problem, and who can they contact if they need more information.

Snedaker and Rima (2013, 401 — 402) talk about external communications. They talk about communications to customers, vendors, shareholders, and media. Customers and vendors need to be notified of the business disruption, the steps that are being taken to rectify the problem, estimated time to recovery, and possible workarounds. If there are shareholders, they must know the nature and extent of the disruption. Communicating with the media is tricky, the plan on what to tell should be well thought and it might be wise to seek legal counsel with regard to what must be disclosed, to whom, and is what time frame.

Elder, J. & Elder, S. (2019, 82) talk about the communication during a disaster. The need to communicate during an emergency occurs immediately, this can mean the difference between success and failure. Different people want different information, and they want it now.

Elder, J. & Elder, S. (2019, 83 – 84) talk about what information should be include in the communications plan. Communications plan includes emergency contact list with contact information for employees, vendors, customers, and other emergency contacts that are deemed fit. Because this information might change it is important to update it regularly. The list should include person's name, cell phone number, email address and contact information of a close member like family.

Elder, J. & Elder, S. (2019, 84) suggest that it is a good idea to create a scripted message for a disaster in advance. Because things can get chaotic during a disaster having a premade template can help in the start of a disaster. It is good to assign one person the responsibility of coordinating disaster communications. This way the messages are more likely to be consistent. It is also important to think about the language of the messages.

Elder, J. & Elder, S. (2019, 86 – 87) communications plans should have different ways to address different groups. Management wants to likely know what happened and when, did anyone get injured, what kind of damage was done, and how long will it take to resume normal operations. An employee might want to know what happened, when is it safe to go back to work, and if they cannot work what will happen. Vendors want to know can deliveries still be made, are orders delayed, are orders cancelled, and are there changes that need to be made.

Snedaker and Rima (2013, 128 — 129) say that in the aftermath of a disaster, the first thing you will need is the information necessary to being recovery. It is important that the documentation is backed up securely and it is readily available off-site. It is also important to review and update this document, to ensure that the documentation is relevant and correct. In order to ensure that all information is available to those who need it in a real disaster, multiple copies are made and stored in different locations.

5.3 Simplified disaster recovery

First part of DRP is the preparation phase. During this phase a company will make three different categories for disasters. These categories are minor disasters, intermediate disasters, and major disasters. After these categories have been created the company will place different disasters in these categories and decide what criteria must filled so that the plan will be put in to action. The company needs to have a document that has everyone’s contact information, so that individuals can be contacted in case of a disaster. This document will contain a person’s name, phone number, email address, and a number of a closed family member. The contact information is gathered so that when there is an incident the individual can be contacted, either thought phone or through email. The number of the closed family member is listed in case the individual cannot be contacted or there has been an accident involving the individual and the family needs to be informed.

During a disaster it is too late to start thinking about how communication should be done, so it is vital to think about what kind of communication documentation needs to be ready and how the communication should be done in case of an incident, both internally and externally. In internal communication it is important that everyone know who are the people that are responsible for communicating. Last thing a company needs during a disaster is three or four different people giving out different information. Someone should be responsible for communications so that it can be ensure that the information that being told is accurate. Communication templates should be created so that when an incident happens correct information can be distributed as fast as possible. Communication templates need to be created for different needs. Other employees need to be receiving different information than the people who are responsible for the recovery. Then there are external communications. If a customer is affected by the incident, they need to also know what is happening and how it is being fixed.

There should be a lot of effort put into backing up documentation in a company. This does not only mean the documentation that is critical to the company's operations but also other documentation like the risk assessment and disaster recovery. These documentations should have backups at multiple different locations. In case on location has an accident affecting the storage, the other location will still have the documentation and it can be restored.

Last part of this phase is training. While having a plan is great, having people who have had a chance to train in case of a disaster is even better. The same way there are fire drills there should be other disaster drills. During this training the company can also see if there are any changes that need to be made into the plan. Training should be done on a regular basis. How often is regular basis is up for the company to decide, because not all companies can train as often as they would like to. But nevertheless, this training should be done. It would be terrible if there is a lot of effort put into a good plan that fails because the company did not put in the effort to test and practice the plan.

Second part of DRP is activation phase. Activation phase comes right after the incident has occurred. In this phase the company will decide if the DRP is activated and what parts of the plan are activated. This phase also includes the initial response to the incident, notification of what has happened, problem assessment, disaster declaration, and plan implementation. Communication between people involved is key to success. Even if there is a flaw in the plan correct communication will help to solve the situation faster.

Third part is the recovery phase. Recovery is phase consists of the steps that are done after the disruption has been stopped or contained. This phase includes removing equipment that can still be saved, assessing the situation, and determining which recovery steps are needed so that operations can return to normal. Communications to customers that are affected and other outsiders about the situation are also done now.

Fourth part is continuity phase. After everything has calmed down and the disruption has been stopped this phase starts. In this phase are the actions that are needed for returning to normal operations. These actions would be ordering and gathering all the pieces and putting them together. Once everything is back to normal, it is time to do documentation of the incident. In order to make sure that recovery is done better in the future it is important to evaluate how the disaster and recovery went, give out criticism to the steps and actions that could have been done better, and develop the DRP. This is when the company moves back to the first phase and starts preparing and training in case of a new incident.

6 CONTINUATION PLAN

6.1 Testing and Evaluation

One way to document and see how a company would handle a disaster right now would be to do excel training. In excel training the participants come up with a target and a disaster, then step by step everything that is needed and how long it takes to do gets listed and at the end of the exercise the company will know how long it will take to fix this disaster.

According to Snedaker and Rima (2013, 149) tabletop can be a way to document and evaluate how a company would respond to a specific disaster scenario. This will give information on how the company operates during disasters and it can be eye-opening for the company doing them.

One example of this exercise would be the following. A company has workstations that are used for designing new products if this workstation cannot be used the production line does not work. The workstation breaks and it needs to be replaced. First 20 or 30 minutes would be used to inform that this incident has happened and trying to figure out can the problem be solved with the current equipment that the company has available. Now it has been determined that the workstation either has to be replaced or it has to go into a repair shop. The repair shop promises that it will have the workstation working in 4 to 6 days. Buying a new workstation would take 1 to 2 days, and after getting a new workstation it will take 1 day to get it installed and working normally. In this simplified example fasted that the company could recover from a loss of a workstation would be 2 days and some hours. In a worst-case scenario, it would take close to a week.

Another way to do exercises that test the ability to recover would be to do a real-life exercise. There are two different types of real-life exercises, one is soft training, and the other is hard training. In these real-life exercises we come up with a scenario, we go to a physical location in the company, and we tell a person to act the scenario out while taking notes and time on how everything goes. The difference between soft and hard exercises is that in soft exercises the actual actions are not done they are just expressed. In hard exercises we act out the scenario and do all the actions that are needed.

An example of a soft exercise would be that a workers workstation catches on fire. First there is the initial response which is to extinguish the fire. The worker would walk to the fire extinguisher and take it to the workstation, but instead of spraying the room with foam the worker will just say that they have extinguished the fire. Next the employee would inform the right contact of what has happened and what has been done so far. The worker would not actually call the fire department but instead the worker would just say that the fire department has been called. After this we would again go through the process on paper to see how long it would take us to get a new workstation and get it working normally.

Soft exercise is also good because it forces the participants to act the situation out as it would be one when it was a real scenario. This type of training can also bring to light other information that was not thought in the start. Does the worker know where the fire extinguisher is located? Does the worker know how to operate the fire extinguisher? Is the fire extinguisher close enough where it is still useful to the situation? It is easy to write on paper I will get the fire extinguisher and extinguish the fire but doing it in real life might be more difficult if it is not practiced.

An example of hard exercise would be that the company tests its backup internet connection. The company has two internet providers, one that provides the main connection and another that is not used unless the first provider is out of use. In a hard exercise the company would do the necessary preparation, call the service provider, ask them to disconnect the service, and see if the backup works. In hard exercises it is important to be 100% sure that this training does not result in loss of data, unplanned damage to the company or danger any individual.

From these exercises the company can do self-evaluation and figure out if there are better ways to recover that would save the company time and money. Is there something we can do speed up the communication and initial evaluation of the situation? Are there any faster ways for us to get new equipment to our location? Should we have a duplicated equipment ready waiting in a storage? Is there something we can change about our company layout or instructions that would result in better outcomes? How much would these fixes cost and how much time would they save?

6.2 Improvement

Snedaker, Rima, and Elders suggested that the documentation should be revisited at least once every year. From this it can be said that the documentation should be visited at least once every year. The documentation should also be updated every time there is a change in the system, or if an incident occurs. If there is an incident and something is discovered it is good to add this discovery to the document immediately rather than waiting for the once per year meeting, because there is a risk that something is forgotten. This will result in only partial improvements from what would be the full potential.

According to Snedaker and Rima (2013, 383) the maintenance phase must occur even if the company never activate the disaster recovery plan. The company needs to review its disaster recovery plan on a periodic basis to ensure that it is still current and relevant. As operations and technology components change and as the company add or change facilities, the company need to make sure that the plan is updated. In addition, if the company end up activating its disaster recovery plan at some point, the company will want to assess the effectiveness of the plan afterward, when things settle down.

A company should update their disaster recovery plan and their risk analysis plan every time there is a change in operations, a new device, a new way of manufacturing a product, a change in leadership or after there has been a disaster. On top of this the company should review its disaster recovery and risk analysis from start to finish at least once every year even if nothing in the plan has changed. By having this much focus on the documentation the company can ensure that the documentations are up to date and everyone who is responsible for something knows of the documentation or at least knows that the documentation exists.

Once the documentation has been done, it is a good idea to focus on improving the testing. For example, if a new risk is discovered the company can test what would happen if this new risk would happen. After the test is done the company can see if there were mistakes that were done during the recovery. If there were some mistakes the company knows where are the areas that need improvement and where to put more focus. If the test went perfectly, the scenario in the test could be made more difficult and there could be more failure points or other negative elements that make the scenario more difficult.

If the company is having difficulties improving their situation it is a good idea to reach out to other companies for help. Services like penetration testing, training, auditing, and other research can be purchased from companies that provide these services. Companies that have good reputation for offering these types of services should be considered even if the company does not think it needs help with improving its situation.

6.3 Training

Everyone who works in the company should be brought to the same basic level of understanding when it comes to the basics in cybersecurity. Some of the basic safety recommendations like locking a workstation or having a strong password, might seem like common knowledge that everyone knows and does. In reality many workers do not follow even the most basic safety recommendations even if they know they should. Usually this is done for convenience or because the importance of these safety recommendations is not known or understood fully. Why should the workstation be locked if the workstation itself is behind a locked door, well it is because of the rare case that the door is not locked. Cybersecurity is not about ensuring that one safety protocol is done correctly and followed, it is about having many different layers of safety so that if one fails the rest will be enough.

Bringing everyone to the same level of knowledge in cybersecurity can be done by making a document that covers the basic. The basics would at least explaining the different security policies that the company has, as well as how to use email and web safely during work. At the start of the employment the new employee must read the document and after this the employee is asked some basic questions to make sure that they have read the document.

Existing employees can be trained by organising cybersecurity training. This can be in the form of a certificate or having in house training. Both options are good and depending on the company one or the other is not better or worse. Another way to do training exercises at the company. Having the employees practice what to do in case of an incident, this can also be used to gather information about what is the level of preparedness at the workplace.

7 CONCLUSIONS

Risk assessment is used to determine what are the most important assets and functions in the company. Once the most important assets and functions are determined the company can better understand and find threats and risks that it is facing. The risk assessment should not be seen as a one and done situation but instead a continues process of updating and improving the current image of the company. When doing risk assessment, it is important to cast a wide net and not only focus on things that are obvious. Gathering information for a wider area will result in a better overall assessment even if the whole process takes a while longer.

Disaster recovery helps the company recover better when it faces a loss in its normal operations because of an incident. Since the company cannot mitigate all the risk and threats that it is aware of it needs a plan on what to do when one of those situations happen. Disaster recovery is a complicated task but dividing it into smaller more easily manageable parts will make the whole process easier to manage. Disaster recovery can also help indirectly even if it does not outright solve the issue. In case something unexpected happens, having partial disaster recovery plan is better than starting from a clean table. Like risk assessment disaster recovery planning should also not be seen as a one and done deal but something that needs updating and practising. Practising disaster recovery is also important. Having a plan is great but having a plan that is practiced and tested is even better.

Overall, it could be stated that risk analysis and disaster recovery are very important for the company. Having knowledge of the company and having a plan on how to return the company's operations back to normal after an incident can mean the difference between the company surviving and having to end its operations forever. It is important to understand that risk analysis and disaster recovery are not just about acknowledging that risk exist and making a plan but also updating and practicing the plan. Since every company is at risk to some type of threats and there will always be threats and risks that can be mitigated it is vital that any company that wants to stay operational for longer than once incident must have a risk assessment and a disaster recovery plan.

8 MEDIATION

When I started this research, I was under the impression that disaster recovery is just about ensuring that the IT systems of the company stay in normal operations and that the risk that face the IT systems are almost all digital. While making this research I found out that majority of the risks are not digital but come from the physical world. Having your mind set on just the digital world when doing risk analysis or disaster recovery plan would be a mistake.

When it comes to the amount of research material, I gathered for this thesis I think that there certainly was enough so that the thesis can be called reliable. The research material was gathered from reliable sources and when I was comparing information it was done by comparing information that came from different sources. Once resource that I could have used would have been the

ISO 31000, since I explained the reason why I did not use this source for this thesis in chapter 3.2 I will not do it again here.

One note that I have about the questionnaire was that the pool of participants was low, only 20 individuals. Usually in questionnaires there is a want and a need for a large base of participants to ensure that the results can be accurate. In my own case I would argue that even that the questionnaire done for this thesis was small it was still accurate information. Typically, questionnaires are sent to individuals at mass, usually through email. While this type of approach can lead to higher number of individuals answering, it will also lead to answers that do not matter. If you send out a questionnaire you must assume that some will not be answered it at all, and some will click through the questionnaire without even thinking about the questions. During my questionnaires I sat down with every single person and asked them the questions personally. I believe that because of this the individuals were more focused on the questions, and they put a lot more effort into the questionnaire. If I would have sent the questions to the individuals over email, I would have gotten a lot of empty answers. By doing the questionnaire the way that I did it the answer rate for the questionnaire was 100% and I believe that the individuals answering were more focused on the questions.

During the questionnaire it would have been interesting to see how the questionnaire changed the cybersecurity view of the person answering. This could have been by having the first and the last question be the same, “do you feel like you would need more cybersecurity training?”. This could have potentially shown how simply talking about the subject can bring more interest into cybersecurity.

REFERENCES

Elder, J. & Elder, S. 2019. Faster Disaster Recovery The Business Owner’s Guide to Developing a Business Continuity Plan. Hoboken, New Jersey, USA. John Wiley & Sons Inc. E-book. Available at: https://ebookcentral.proquest.com/lib/xamk-ebooks/reader.action?docID=5741229&query=Business+Continuity [Accessed 2 May 2023].

Empiirinen tutkimus. 2015. Jyväskylän yliopisto. WWW document. Updated 23 March 2015. Available at: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/empiirinen-tutkimus [Accessed 2 May 2023].

Laadullinen tutkimus. 2015. Jyväskylän yliopisto. WWW document. Updated 23 March 2015. Available at: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/laadullinen-tutkimus [Accessed 23 August 2023]

Monimenetelmällisyys. 2021. Jyväskylän yliopisto. WWW document. Updated 25 August 2021. Available at: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/monimenetelmaisyys [Accessed 23 August 2023].

Määrällinen tutkimus. 2015. Jyväskylän yliopisto. WWW document. Updated 23 March 2015. Available at: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/maarallinen-tutkimus [Accessed 2 May 2023].

Shostack, A. 2007. STRIDE chart. Microsoft. WWW document. Available at: https://www.microsoft.com/en-us/security/blog/2007/09/11/stride-chart/ [Accessed 22 November 2023].

Snedaker, S. & Rima, C. 2013. Business Continuity and Disaster Recovery Planning for IT Professionals. 225 Wyman Street, Waltham, MA 02451, USA.

Elsevier Inc. E-book. Available at: https://ebookcentral.proquest.com/lib/xamk-ebooks/reader.action?docID=1115178&query=Business+Continuity+and+Disaster+Recovery+Planning+for+IT+Professionals [Accessed 2 May 2023].

The importance of disaster recovery plans for businesses. 2022. Vodafone. WWW document. Updated 23 April 2021. Available at: https://www.vodafone.com/business/business-resilience/importance-of-disaster-recovery-business-plans [Accessed 2 May 2023].

Townsend, R. 2022. What is a Disaster Recovery Plan and Why is it Important? Nexstor. WWW document. Updated 31 August 2022. Available at: https://nexstor.com/what-is-disaster-recovery-plan/ [Accessed 2 May 2023].

Vetikko, P. 2019. What is the ISO 27001 standard? Insta. WWW document. Available at: https://www.insta.fi/nakemyksia/tietoturvapalvelut/mika-on-iso-27001-standardi [Accessed 2 May 2023].

What is a Disaster Recovery Plan? Google Cloud. WWW document. Available at: https://cloud.google.com/learn/what-is-disaster-recovery [Accessed 2 May 2023].

Appendix 1

1. Do you think that you would be able to know the difference between a scam email and a regular email?

2. Is there a plan on what to do in case your section has a cyber incident?

3. Do you know the person you need to contact in case of a cyber incident?

4. Has an IT incident happened while you have been working here?

5. Have you been trained in what to do in case a cyber incident happens, that would prevent you from doing your normal work?

6. Do you know what you are supposed to do if you have a cyber incident?

7. Have you ever had malware on any of your devices either at work, school, or home?

8. Do you have recurring training regarding cybersecurity at your workplace?

9. Have you ever been trained in basic cybersecurity, for example how to use email safely at work?

10. Do you feel like you would need more cybersecurity training?

11. Is your password longer than 12 characters?

12. Do you always lock your workstation when you leave it, even if it is just for a short time?

Appendix 2

Theme 1: Assets and functions

1. What are the assets and functions that your company might have?
2. What are the most critical assets that ensure normal operations in your company?
3. How is cybersecurity training done in your company?

Theme 2: Risk tolerance

1. How much can a cybersecurity incident cost for your company?
2. How long can critical functions be out of use for your company?

Theme 3: Disaster recovery

1. How is your company prepared in case of a cyber incident?
2. How does your company train for a cyber incident?
3. How does your company do its internal and external communication in case of a cyber incident?
4. How should your company divide its different responsibilities in case of a cyber incident?
5. Have you ever experienced a cyber incident?

Theme 4: Importance of cybersecurity

1. How do you view the importance of cybersecurity when we are talking about the company’s assets and functions?
2. Has there been audits or other research that would show improvements in your company’s cybersecurity?
3. What is your understanding of how the workplace as a whole sees cybersecurity? Is it seen as important or not?