The Black Swan, Prepare for Survival

Are Companies Prepared for
Massive Disruptive Cyber Threats

Michiel van der Steeg
S2465132

08-01-2020

Master Thesis

Dr. Tommy van Steen

18511 words

Table of Contents

Introduction

Over the last few years cyber threats have been evolving. Ransomware attacks for example, grew 118% in the first quarter of this year (McAfee, 2019). However, there is one kind of threat that deserves special attention: The Black Swan. Black Swan is a term used in risk management to indicate events which are considered exceptions with severe impact, or events for which people cannot assess the risk they pose or anticipate on. (Taleb 2007, as quoted by Paté-Cornell, 2012).

In this case of cyber threats, the Black Swan is seen as a cyber threat with highly disruptive powers and the capability to spread massively across networks. These threats possess the ability to stop business continuity and bring the survival of the targeted corporation in danger. This research will see a Black Swan as a massive disruptive cyber threat.

An example of such a Black Swan is the NotPetya malware, the costliest cyber attack to date (Kaspersly Lab, 2018). NotPetya was malware which was uploaded into M.E. Doc, a Ukrainian accounting software company, before spreading towards its intended targets. The global shipping company Maersk was one of the targets which became infected and their complete infrastructure was damaged. The only reason why they were able to recover was because a blackout in Ghana had knocked a computer off the network. This computer still contained the only copy of the company's domain controller which was not harmed by the malware (Greenberg, 2018).

If it was not for the blackout, Maersk would not have been able to recover from this attack. Despite their survival, they still suffered damages of $300 million in costs from the attack which nearly bankrupted the company. Maersk was not the only company affected. The White House has estimated that the total damages of this massive disruptive cyber threat ran up to 10 billion dollars (Greenberg, 2018).

Because of the increasing size of the attackable digital surface of companies, these threats are becoming harder to detect and to respond to. The report of the Scientific Council for Government Policy (WRR, 2019) shows that the government has not got enough resources to deal with these threats, especially when these have disruptive consequences. Since the government fails to deal with these threats, companies need to prepare themselves for these black swans and try to become more cyber resilient.

The aforementioned report also states that because of digitalization, public facilities have become privatized. Companies and government bodies are outsourcing digital support to third parties, for example digital service and cloud providers. Dependence on these third parties can bring the company in danger as well. If one of these third parties is not well prepared for such an attack, the company and the government bodies who are using their services, bear the consequences (WRR, 2019). For example, Maersk was infected through its accounting software, which provided to them by a third party. (Greenberg, 2018).

Imagine scenarios where the supply chain and logistics of companies and their third parties are completely disrupted. As seen in the survival of Maersk, most business continuity and disaster recovery models rely on assumptions which will be invalidated when a massive disruptive attack occurs. Therefore, the cyber resilience of companies needs to be researched at the hand of these models.

Lately, more reports have been published regarding this subject. For example, the report by the Scientific Council for Government Policy "*Prepare for Digital Disruption"* (WRR, 2019) and the report of the NCSC "*Cyber Security Assessment Netherlands"* (2019). This shows that the topic is becoming more and more relevant.

In addition to this upcoming relevance, this research is academically relevant because the field of cyber security often focusses on massive disruptive threats regarding states instead of towards companies for example as in Rid's article Cyber War Will Not Take Place (2012), where he discusses massive cyber threats in regard to states. Looking at these threats from the perspective of companies is a new angle which needs to be taken into account.

Another place where this research finds its academic relevance is Risk Management. When this paper researches business continuity and disaster recovery models, it enters the domain of risk management. In the academic literature of risk management, there are some articles which take into account massive disruptive threats, for example, 'Integrated business continuity and disaster recovery planning: Towards organizational resilience' by Sahebjamnia et al (2015). However, this article does not look at disruptive cyber threats specifically, they only research other disruptive threats. This will further be discussed under the body of knowledge.

To research these massive disruptive threats and the cyber resilience of companies, this thesis will set out to answer the following research question: '*To what extent do companies take into account massive disruptive cyber threats in regard to business continuity and business survival, and how can companies prepare themselves to make them more cyber resilient?*' My hypothesis is that massive disruptive threats are not taken into account, companies underestimate these threats and expect not to be targeted, or underestimate the scope of collateral damage. These companies need to upgrade their current business continuity and disaster recovery models to face future cyber threats. *"Boosting resilience is the most important tool in reducing risk"* (NCSC, 2019, p6).

To answer this research question, this thesis will set out the following sub questions:

- *What are massive disruptive cyber threats?*
- *How do companies see massive disruptive cyber threats and how are they prepared to deal with such threats?*
- *What does business continuity and business survival mean for the researched companies and what should a relevant business continuity and disaster recovery plan look like?*

In the next few chapters this research will set out to explore the cyber resilience of companies in regard to massive disruptive cyber threats. NotPetya has proved that there are Black Swans under the cyber threats which are capable of bringing the survival of the targeted company in danger. The report of the Scientific Council for Government Policy (2019) stated that the government is not ready to stop these threats, therefore companies need to become more cyber resilient themselves. Since there is no literature on the cyber resilience of companies and their business continuity and disaster recovery plans in regard to massive disruptive cyber threats, this research will aim to fill that gap. The next chapter will position this research in the body of knowledge available.

Body of Knowledge

This research fits in with crisis and security management. The research takes place in one of the emerging fields in this sector; cyber security. "*Cyber security refers to the entirety of the measures to prevent damage caused by disruption, failure or misuse of ICT and to repair it should any damage occur. This damage could consist of impairment of the availability, confidentiality or integrity of information systems and information services and the data contained therein"* (NCSC, 2019, p. 8).

Since this research specifically focusses on large companies, it is difficult to find an existing framework which is relevant. A lot of the literature regarding massive disruptive cyber threats sees the state as the main target (Rid, 2012). While most theoretical frameworks regarding the prevention of such a threat focus on security hygiene through security awareness training (Stanton et al, 2005) and on identifying the most important data of the corporation. Allodi and Massacci (2017) have set out an "Information Security Risk Management Process". Which exists out of the following steps:

- Asset and process identification
- Business impact analysis
- Risk assessment
- Security requirements identification
- Risk treatment

This theoretical framework assumes that it is possible to prevent a massive disruptive threat. However, no matter how high the level of the security of the company, the company should always assume that the current security countermeasures are not sufficient to properly detect and prevent massive disruptive threats. Therefore, it is important to have a good response plan in place.

Since there is no academic literature on the cyber resilience of companies in regard to massive disruptive cyber threats, this research will aim to fill that gap. However, since this thesis will research the resilience of companies during a cyber crisis at the hand of business continuity and disaster recovery frameworks, it also takes place in the field of risk management. There is academic literature regarding disruptive threats in the field of risk management, however, not regarding massive disruptive cyber threats.

For this research massive disruptive threats are seen as a "Black Swan". The use of this metaphor has been rising in the field of risk management. It is an appealing comparison to define unpredictable events. Taleb (2007) is the instigators of this trend. He attributes three characteristics to the black swan. 1.) It lies outside our regular perspective. 2) The consequences of such an event are severe. 3). After the event has happened, the event becomes explainable.

Aven (2012) studies the black swan at the hand of four relatable interpretations. "*1. A surprising extreme event relative to the expected occurrence rate (extreme event in the sense that the consequences are large/severe, this understanding also applies to the interpretations 2 and 3 below).*

2. An extreme event with a very low probability. 3. A surprising, extreme event in situations with large uncertainties. 4. An unknown unknown" (Aven, 2012, p. 45).

The first interpretation is an unexpected event relative to the chance of it happening, with extreme consequences. Aven (2012) concludes it is difficult to define an event as a black swan solely at the expected rate of occurrence. He states that "*Considered in isolation, one type of extreme events may be considered surprising but not if we open up for all types of events*" (Aven, 2012, p. 45).

Regarding the interpretation that the extreme event has a low probability he comes to the same conclusion. He argues that probability can be based on assumptions, which are not always correct since in most cases, not all information is available. Therefore, to conclude that an event is a black swan based on the probability is incorrect according to Aven.

The black swan as an event in situations with large uncertainties, is a more coherent interpretation. In the face of uncertainty, it is difficult to predict events since there is no reference for what can or will happen.

Finally, the interpretation of a black swan as an unknown unknown. Aven (2007, p. 47) states that "*a reasonable interpretation of this statement is that if the risk description of the risk assessment is not able to capture the event, it is an unknown unknown and a black swan – nothing in the past can convincingly point to its possibility, interpreting the past in a wide knowledge sense.*"

Aven (2007, p. 47) concludes that there are two possible interpretations of the black swan concept: "*(i) as a rare event with extreme consequences, or as a term for expressing (ii) an extreme, surprising event relative to the present knowledge.*" He argues that interpretation (ii) should be employed since interpretation (i) consists out of a large group of events including those which are extraordinary but understood. Finally, he gives the conclusion "that a black swan is to be seen as a surprising extreme event relative to the present knowledge/beliefs" (Aven, 2012, p. 49).

This research will define a black swan as both possible interpretations, 'a surprising event relative to the present knowledge with extreme consequences'. The reason for the combination of the interpretations is that the consequences are very important to classify something as a massive disruptive cyber threat. Next to that, the relevance to the present knowledge is difficult to conclude. Most cyber security experts are aware of the entire threatscape, but the researched companies will have limited knowledge, therefore making more events black swans. Therefore, a combination of the interpretations is necessary and a black swan will be interpreted as a surprising event relative to the present knowledge with extreme consequences.

To analyze how companies can make themselves more cyber resilient this research will aim to create a framework which will help them doing so. To create this framework, existing articles regarding business continuity frameworks are analyzed. The following articles will be analyzed: 1.) Business Continuity Planning: A Comprehensive Approach (Cerullo & Cerullo, 2004), 2.) A Framework for Business Continuity Management (Gibb & Buchanan, 2006) and 3.) Integrated Business Continuity and Disaster Recovery Planning: Towards Organizational Resilience (Sahebjamniaa et al, 2015).

The article by Cerullo and Cerullo describes that the risk of business disruption increases when the dependence on information technology increases. The aim of the article is to give insight in the state of business continuity plans. According to them (2004, p. 70), "*a comprehensive approach to business continuity planning seeks to mitigate against all major business interruptions of business systems*."

The article states that every company can be harmed by disasters, either natural or cyber related. In the research Cerullo and Cerullo (2004) did, they found out that of the businesses which were damaged by Hurricane Andrew in 1992, 80% of the businesses without a business continuity plan (BCP) did not recover and went out of business. They stress that BCPs are necessary to recover from business disruption. Next to this, they also stated that the risk has expended as well due to the increased IT dependences, the links to external networks and the rise of cyber threats.

Cerullo and Cerullo state that there should not be a single framework for business continuity, but that it should be designed for every unique situation. They argue it should be able to change with the changing risks, business capabilities and technological developments.

However, according to them a BCP should contain the following elements*: "1. Identify major risks of business interruption. 2. Develop a plan to mitigate or reduce the impact of the identified risk. 3. Train employees and test the plan to ensure that it is effective"* (Cerullo & Cerullo, 2004, p. 71).

Gibb and Buchanan (2006) aimed to create a framework for business continuity management (BCM) within the context of an information strategy in their article. They argue that the risk for businesses increases through natural disasters but also through the increasing dependence on information technology and failure of the underlying systems.

"Business continuity management (BCM) is a tool that can be employed to provide greater confidence that the outputs of processes and services can be delivered in the face of risks" Gibb & Buchanan, 2006 p. 129). This tool is used to manage and identify risks, control the impact of the risks and increase the success rate of recovery. Figure 1. shows their proposed BCM.

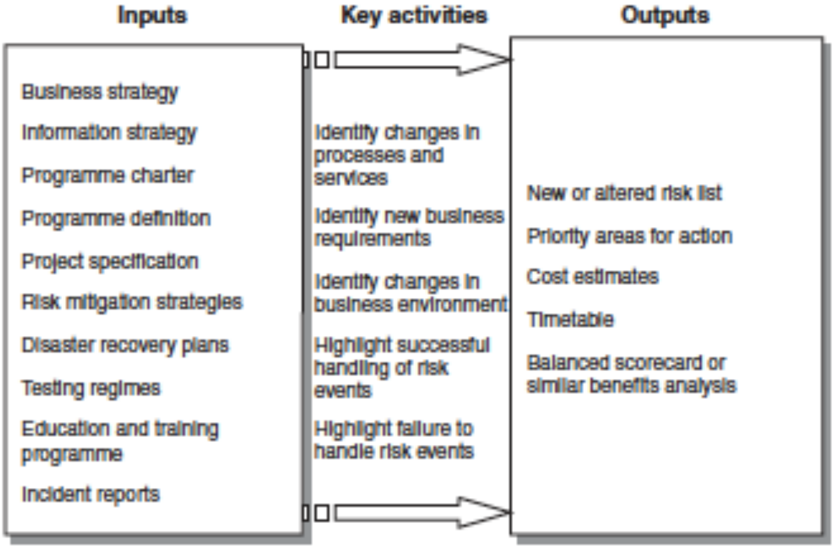

Inputs
Key activities
Outputs
Business strategy
Information strategy
Programme charter
Programme definition
Project specification
Risk mitigation strategies
Disaster recovery plans
Testing regimes
Education and training programme
Incident reports
Identify changes in processes and services
Identify new business requirements
Identify changes in business environment
Highlight successful handling of risk events
Highlight failure to handle risk events
New or altered risk list
Priority areas for action
Cost estimates
Timetable
Balanced scorecard or similar benefits analysis

Figure 1. (Gibb & Buchanan, 2006, p. 140)

The BCM proposed by Gibb and Buchanan exists out of the following nine phases, *“1. Programme initiation. 2. Project initiation. 3. Risk analysis. 4. Selecting risk mitigation strategies. 5. Monitoring and control. 6. Implementation. 7. Testing. 8. Education and training. 9. Review”* (Gibb & Buchanan, 2006, p.129).

In the first phase, the program initiation, a senior manager should induce the development of the BCM and allocate the resources to create the BCM. This program should contain who should run the projects and when they will be initiated. The second phase is the project initiation. In this phase the proposed projects should be started following regular project management methodologies.
The third phase is risk analysis, which can be classified in the identification of risks, the evaluation of risks and a business impact analysis. After this phase is completed, it is important to move on to the mitigation strategies. These can be divided in strategies which deal with the risks before they occur and strategies which deal with the risks after they occur. The monitoring and control phase overlaps with the following phases. It takes the implementation of the BCM, the testing and the education and training into account. Finally, after the testing it is important to review the BCM to see if it suffices (Gibb & Buchanan, 2006).

Sahebjamniaa et al. (2015) state that businesses are running into more risks of disruptions. They state that companies need to protect themselves from these risks with a proactive approach. Their article sets out a decision support framework to help companies prepare themselves for these risks. This framework was designed to “control the loss of resilience by maximizing recovery point and minimizing recovery time objectives” (Sahebjamniaa et al, 2015). Sahebjaamniaa tests the model against the following disruptive events: an earthquake, flood, fire, personnel sabotage and epidemic diseases (2015).

Firstly, they give an example of a regular Integrated Business Continuity and Disaster Recovery Planning, (IBCDRP) figure 2.

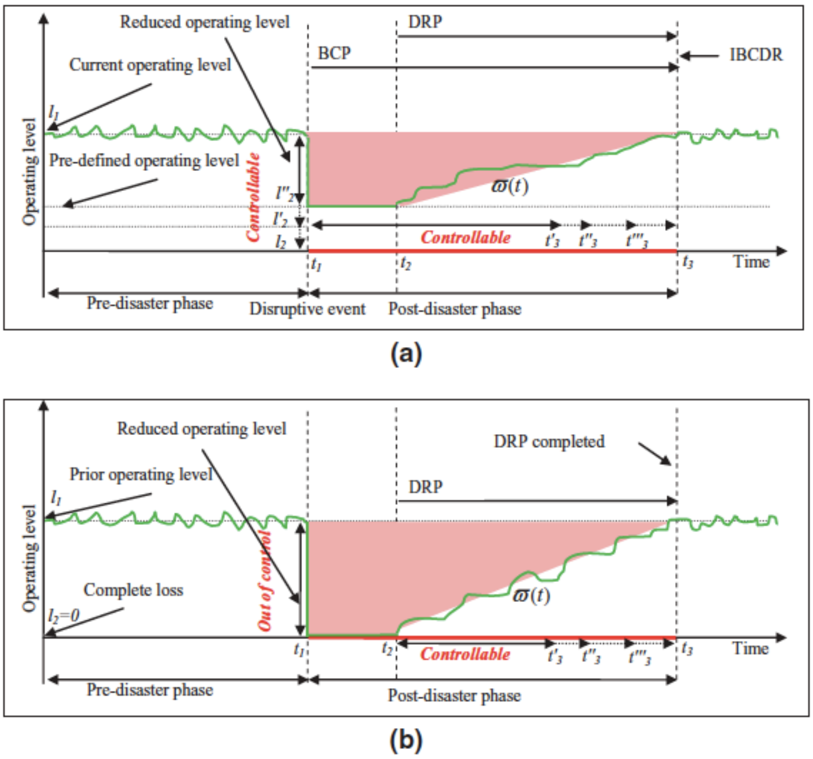


Figure 2 (Sahebjamniaa et al, 2015, p. 263)

Their critique on the regular model is that the BCP starts when the disruptive event occurs, and the DRP starts when the disruptive event has ended. Therefore, they aim to improve upon this model, "*the developed IBCDRP framework should be able to make and validate an integrated continuity and recovery plan for the organization's critical operations not only before, but also during and after any disruptive event by arranging required resources in advance" (*Sahebjamaniaa et al, 2015, p. 263).

In figure 3. you see the proposed IBCDRP model of Sahebjamniaa et al. (2015). This model addresses the problems on three different levels: Strategic, Tactical and Operational.

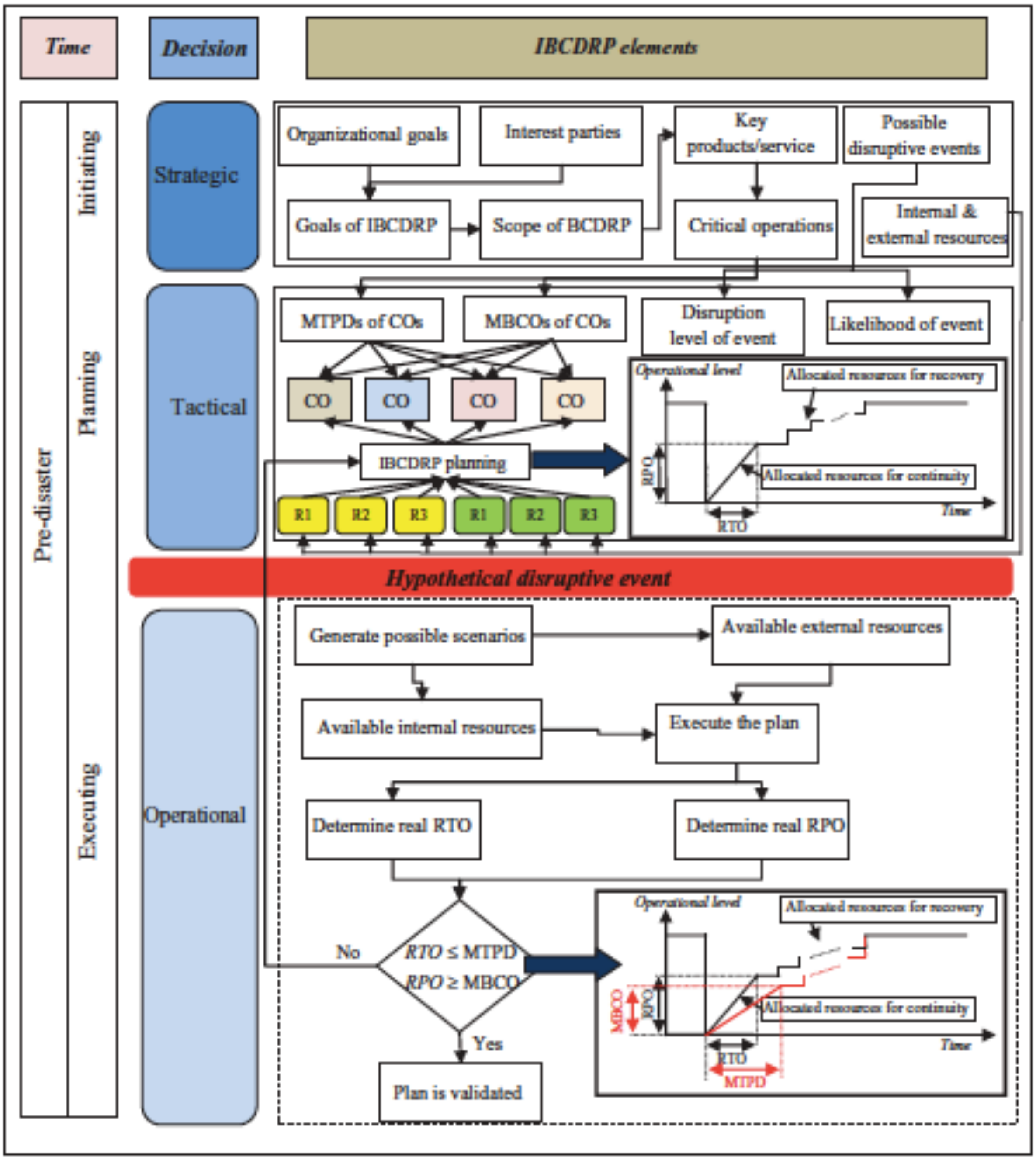


Figure 3 (Sahebjamniaa et al, 2015, p. 264)

At the Strategic level, the goal of the framework for the specific company is formed, the critical operations (CO's) are listed, and the company's resources are identified. Next to the business, the chance of it happening and the kind of disruptive events which could occur will be examined as well.

At the Tactical level, the CO's are analyzed. The minimum business continuity objective (MBCO) and the maximum tolerable period of disruption (MTPD) of the CO's are defined.*"*

The Operational level is about testing. This model proposes to test the effectiveness of the plans with simulated hypothetical disruptive events. If these plans are in accordance with the MBCO and the MTPD the framework will be validated, if not changes are to be made at the tactical level.

This thesis aims to create a framework which will help companies make themselves more cyber resilient. Therefore, it will use the information obtained out of the above discussed articles and the information out of the result of the research to create such a business continuity plan and disaster recovery plan.

The article of Cerullo and Cerullo acknowledges the risk of cyber threats. They do not propose a business continuity framework. According to them "*there is no single recommended plan for business continuity; instead, every organization needs to develop a comprehensive BCP based on its unique situation"* (Cerullo & Cerullo, 2004, p.71).

Despite the fact that they do not propose a specific framework, they do propose three elements which should be included in a BCP, the identification of the risks, the developing of a plan to reduce the impact of the risk (a disaster recovery plan) and the training of employees and testing of the plan.

The article by Gibb and Buchanan (2006) also stressed the risk the increased dependence on information systems brings. This article did propose a business continuity model existing out of nine phases. The nine phases are sufficient to prepare a company for business risks, the fourth phase also mentions that a plan should be made to reduce the impact of the risk afterwards, however, this BCM does not elaborate enough on disaster recovery.

Finally, the article of Sahebjamniaa et al. (2015) proposes the IBCDRP framework which takes into account business continuity management and disaster recovery. However, this framework is not designed to deal with disruptive cyber threats. Therefore, this research will build upon the IBCDRP framework by Sahebjamniaa et al. (2015) and update the framework to make it compatible with massive disruptive cyber threats.

Methodology

To answer the research question: '*To what extent do companies take into account massive disruptive cyber threats in regard to business continuity and business survival, and how can companies prepare themselves to make them more cyber resilient?*' this research will make use of content analysis and interviews. It will propose an upgraded version of the IBCDRP framework (Sahebjamniaa et al, 2015) which companies can use to become more cyber resilient.

Content analysis is best suited for the first part of this research which will answer the first sub question *"What are massive disruptive cyber threats?"* at the hand of threat reports of cyber security firms from the last two years. My assumption is that the biggest threats entail ransomware, malware, phishing, cyber physical, Botnet, IoT, DDoS, Supply chain attacks and third-party attacks. These are threats which are able to stop business continuity and bring the survival of the targeted corporation in danger, existing countermeasures have limited to no effectiveness and the implications will have bigger impact on society than only the targeted organization.

This research will also look into the attackers behind these threats: Individuals, hacktivists, hack syndicate, states and cyber crime proxies and try to define the break-out time per attack. There are several outstanding cyber security firms which bring out reports about the biggest cyber threats every year. These reports will be analyzed to define what massive disruptive cyber threats entail and bundle them together in a threat matrix. This matrix will show what the threats are, what the actors are behind the attacks and what break-out time is average.

The categories which will be analyzed from the reports are: cyber threats, threat actors, scope of the threat and the break-out time. "*A cyber or cybersecurity threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general"* (Taylor, 2018*).* The threat actors will be defined as actors preparing and carrying out cyber attacks against targeted companies. The scope of the threat will be defined as the potential impact of the treat. Does disrupt society or does it harm business continuity and bring the survival of the targeted company in danger? The last category which will be used for analysis is the breakout time. Breakout time is "*the speed with which adversaries accomplish lateral movement in the victim environment after their initial compromise* (Crowdstrike, 2019, p. 14). These four categories are chosen since they determine what kind of threats are active at this time, who are posing these threats, what kind of damage these threats can do and in what time period, therefore indicating massive disruptive cyber threats.

The categories are found by looking for their indicators in the reports. The indicators do not need to be found literally, if the reports refer to an indicator this will be taken into account as well. A discussion on one of the indicators will suffice as well. The following sentence is an example of a paragraph which contains the indicators for the category 'Cyber Threat'. The indicators for these category is that it can include statements about malicious acts which seek to damage data, it can include statements about malicious acts which seek to steal data and that it can include statements about malicious acts which seek to disrupt the digital infrastructure of a company.

Additional evidence of a changing eCrime ecosystem came from prolific ransomware-as-a-service (RaaS) adversary PINCHY SPIDER (GandCrab) and the solidification of MUMMY SPIDER (Emotet) as a professional malware distribution operation.

Since the paragraph refers to 'ransomware-as-a-service' and to 'a professional malware distribution operation', services and operations which seek to damage data and disrupt the digital infrastructure of a company, this paragraph is categorized under the category 'Cyber Threat'.

The codebook which provides these indicators is attached in the Annex and the coding sheet will be attached in the zip file.

The unit of analysis this research uses is paragraphs. Paragraphs are chosen instead of sentences since the threats are mostly defined in entire paragraphs and not sentences. Depending on the document the choice has been made what to analyze, it is detailed in the coding sheet. In general, the entire reports have been analyzed expect for case studies, recommendations and the about the company section. In the Accenture Security (2019) report, only the executive summary is analyzed, the rest of the report was filled with examples of accidents and case studies. It contained too much details and not enough data to analyze. The analysis done is a combination between quantitative and qualitative analysis.

The best way to get more information about the second sub question *"How do companies see massive disruptive cyber threats and how are they prepared to deal with such threats?"* is by conducting interviews with several of these companies. The goal of these interviews is to find out what their view on cyber threats is, what the trends are in the cyber threat landscape and how their business continuity and disaster recovery plans work. At the hand of that data this research will analyze if those plans will be sufficient to deal with these threats. This research conducted four different interviews. All the interviews will be anonymized. The following organizations will be interviewed 1) a government body, 2) a consultancy, 3) a cyber security firm and 4) a logistics service provider in the supply chain of retail businesses. The interview with the expert from the government body was conducted by telephone. It lasted 23 minutes and the transcript consists out of four thousand words. All other interviews were conducted face to face. The interview with the consultancy lasted 42 minutes and the transcript consists out of seven thousand words, the interview with the cyber security firm expert lasted 51 minutes and the transcript consists out of eight thousand words and the interview with the IT director of the logistic service provider lasted 35 minutes and the transcript consists out of five thousand words.

The indicators for the interviews will be cyber threats, threat actors, scope of the threat and cyber resiliency These indicators aim to help to find out what these companies see as the biggest threats, how they expect the cyber threat-landscape to evolve, how they would have handled previous threats and how they are prepared for future threats.

. The indicators need to be discussed to be highlighted. Answers given by the interviewee have to be specifically pointing to that indicator for it to be highlighted. A simple mention of the indicator is not enough to be highlighted. The highlighted transcripts are to be found in the appendix. The interview questions are attached to the appendix as well.

After the planned interviews, this thesis will answer the third sub question: *"What does business continuity and business survival mean for the researched companies and what should a relevant business continuity and disaster recovery plan look like?"*

In the above-mentioned interviews, this research will also aim to figure out the organizational resilience of the companies, if they have business continuity and disaster recovery plans in place and if so, what these plans entail.

Finally, an assessment will be made to see if the companies and the measures they have taken can guarantee business continuity and business survival. My hypothesis is that these measures do not suffice when they are the victim of a massive disruptive cyber threat. History shows that when these threats occur, companies suffer massive damages and have no or insufficient measures in place. For example, companies were not prepared to be infected by something like NotPetya, which resulted in estimated damages totaling over 10 billion dollars (Greenberg, 2018). Therefore, to answer the research question: *'To what extent do companies take into account massive disruptive cyber threats in regard to business continuity and business survival, and how can companies prepare themselves to make them more cyber resilient?'* this research sets out to create an upgraded model of the IBCDRP (Sahebjamniaa et al, 2015) in order to provide the companies with a business continuity and disaster recovery model which will make them more cyber resilient. The model of Sahebjamniaa (2015) focusses on disruptive events, however, it has not been tested in the light of a disruptive cyber event. Therefore, the model needs to be upgraded to in relation to cyber resilience.

Since this research exists out of content analysis and interviewing companies, it will rely on both primary sources from the companies and secondary sources, for example the threat reports of the cyber security firms which will be used for the content analysis. The research will use an inductive approach to gather data, look for patterns and develop upon the IBCDRP framework. It will use desk research for the content analysis to create the threat matrix. which is used in the interviews. Latent coding will be used to analyze the interviews. The interviews will mostly consist out of open questions and will be semi-structured. The research will use an idiographic approach. This approach is one within social research that focuses on specific elements and is mostly used for theory building as the goal of this research is building upon an IBCDRP framework.

The validity of the research should also be analyzed. There are threats to the validity of the research. When interviewing the companies, instead of finding out the measures they have implemented to counter these threats and if they are prepared against such threats, the companies can use the research to find out what kind of measures are useful to implement. So instead of learning what the corporations use, the corporations learn what they should use.

Massive Disruptive Cyber Threats

To answer the sub question: "*What are massive disruptive cyber threats?*" this research made use of content analysis. My expectation is that the reports will show that the biggest threats entail ransomware, malware, phishing, cyber physical, Botnet, IoT, DDoS, Supply chain attacks and third-party attacks. These threats have the ability to bring the business continuity and survival of the company in danger. This expectation comes from looking at previous massive disruptive cyber threats such as the WannaCry and the NotPetya cyber attacks.

The data regarding massive disruptive cyber threats can be found in government reports (for example from the NCSC), reports from police organizations (for example Interpol / Europol), cyber threat reports by cybersecurity firms, cyber threat reports from consultancies and media outlets (trustworthy newspapers and news programs). This research has chosen to focus on government reports and reports from cybersecurity firms and consultancies. This choice has been made, since these reports are all written by experts in the field. They provide the most accurate data on cyber threats and attacks in the last years, since the writers have helped stop these attacks or helped companies recover from these threats. The reports that are chosen are published yearly or quarterly, all have been published in 2018 or 2019. The reason for this timeframe is that the cyber threat landscape is evolving, every year new threats arise and old threats vanish. To research the current biggest threats, reports should be analyzed which are up to data and written in the last two years. Concluding, these reports contain the most relevant data regarding massive disruptive cyber threats.

It is relevant to research these reports since they have been written by the industry experts. By analyzing these reports, this research will find the present cyber threat landscape as perceived by the industry experts. After the analysis of the reports, the findings will be compared to the findings which will come out of the expert interviews. A comparison will be made to see if the reports are up to date, miss data or provide threats which the experts do not deem relevant.

The following documents are analyzed:

Company	Report	Core Business
CrowdStrike	Global Threat Report: Adversary Tradecraft and the Importance of Speed (2019).	Endpoint protection, threat intelligence and response services.
CrowdStrike Services	CrowdStrike Services Cyber Intrusion Casebook 2019: Stories from the Front Lines of Incident Response in 2018 and Insights that Matter for 2019.	Endpoint protection, threat intelligence and response .services.
National Coordinator for Security and Counterterrorism	Cyber Security Assessment Netherlands CSAN 2019.	Increasing the resilience in the digital domain of the Netherlands.
McAfee	McAfee Labs Treats Report, August 2019.	Providing consumers and companies with advanced cyber security solutions.

Check Point Research	Cyber Attack Trends Analysis Key Insight to Gear up for in 2019: 2019 Security Report Volume 01.	Cyber threat intelligence.
Symantec	Internet Security Threat Report Volume 24 | February 2019.	Provides security products and solutions to protect businesses from cyber threats.
Accenture Security	Cyber Threatscape Report (2019).	Consultancy

Table 1.

The categories which will be analyzed from the reports are: cyber threats, threat actors, scope of the threat and the break-out time. These four categories are chosen since they determine what kind of threats are active at this time, who are posing these threats, what kind of damage these threats can do and in what time period, therefore indicating massive disruptive cyber threats.

The categories are found by looking for their indicators in the reports. The indicators do not need to be found literally, if the reports refer to an indicator this will be taken into account as well. A discussion on one of the indicators will suffice as well. The following section will summarize the findings from the articles by the four categories after which it will aim to answer the sub question: “*What are massive disruptive threats?”*

Cyber Threats

CrowdStrike has seen a rise in state sponsored cyber espionage operations. They state that these operations are often precursors to destructive operations. The NCSC also stated that digital resources are being used for espionage and even sabotage by nation-states more frequently. McAfee also described the threat of cyberespionage campaigns, which target national security think tanks. All three of these actors agreed that espionage operations were induced by state actors.

Next to the espionage operations, CrowdStrike identify malware as one of the biggest threats. “*CrowdStrike analysis continues to identify malware as a dominant method used by various types of attackers for initial infiltration*” (CrowdStrike, 2019, p. 16). Check Point Research even reports that malware is becoming more functional. “*Malware families previous known for their single, well-functioning utility are now expanding their operations and offering additional capabilities. Furthermore, new malware families are often released to the wild with more than one significant goal or attack vector*” (CPR, 2019, p.14). For example, as hybrid assault which exists out of banking malware, cryptominers and botnet attempts. CrowdStrike agrees that the intrusion through malware will often lead to more advanced techniques, for example deploying bots for DOS operations, cryptojacking, stealing login credentials to banking sites through banking malware or for the: ““*living off the land” tradecraft that uses legitimate tools already present on the target system to accomplish adversary objectives*” (CrowdStrike, 2019, p. 12). CrowdStrike (2019, p. 23) concludes that “*While malware remains a significant component of modern attacks, it generally comprises only a portion of an overall attack campaign.”* As well as CrowdStrike, the NCSC mentioned the increase of the “living off the land” attacks. The NCSC especially voices their concern about nation-state actors using this attack. Symantec also reported on “Living off the land”. Symantec sees an increase in this type of attack and states it is being used more frequently in targeted attacks since it helps attackers maintain a low profile by hiding in a mass of legitimate processes. Accenture Security also describes the increase in the usage of the “living off the land” tools.

Another change in the cyber threat landscape CrowdStrike noticed was the rise in crimeware distribution. Ransomware-as-a-service made its way into existence and criminal groups set themselves up as professional malware distribution operations. CrowdStrike Services noticed this trend as well. They saw a rise in commodity malware. “*Commodity malware is often a precursor to a disruptive attack. Access gained with commodity malware is increasingly sold to other bad actors, who use it to deploy ransomware, steal intellectual property, or engage in cryptomining, fraud, and extortion*” (CrowdStrike Services, 2018, p. 4). This was also seen in a malware family called TrickBot. After it gained access it handed it over to other groups who undertook ransomware attacks. In accordance with CrowdStrike and CrowdStrike services, the NCSC also points out that digital crime has become much easier because of Cybercrime-as-a-service. “*Cyber attack capabilities can be easily obtained via commercial providers and via the substantial cyber criminal services sector”* (NCSC, 2019, p. 12). Next to commodity malware, cybercrime-as-a-service also includes hiring the service of cyber attackers, who according to the NCSC (2019, p. 18) *“frequently offer Dutch ICT infrastructure as part of their services*.” Check Point Research also reports on this threat, they describe it as an affiliate system for non-technical criminals to also profit from this digital form of attack. They add access to corporate networks is for sale, attackers can use this access to release ransomware on a corporate wide scale.

Alongside the rise of ransomware-as-a-service, CrowdStrike identified the continued rise of “Big Game Hunting” as the most noticeable trend in 2018. ““*Big Game Hunting” refers to eCrime operations using ransomware to target large organizations for a high return. Often, these sophisticated campaigns include well-tested reconnaissance, delivery and lateral-movement TTPs*” (CrowdStrike, 2019, p. 51). (TTP’s stands for Tactics, Techniques, Procedures). The goal of Big Game Hunting is to extract large ransom amounts from specific organizations. CrowdStrike Services also noticed that ransomware attacks have evolved. They stated that besides big game hunting, some ransomware attacks are making use of bot networks to deliver and spread the infection. This malware is designed to spread to any system connected with it. The NCSC on the other hand stated that there has been a decline in ransomware in the Netherland. *“Businesses appear to be better prepared to recover data following infections of ransomware, resulting in fewer ransoms being paid”* (NCSC, 2019, p. 27). However, they do agree with CrowdStrike that there is an increase in targeted ransomware attacks, described by CrowdStrike as big game hunting. McAfee states that after the decline of ransomware attacks in 2018, the first quarter of 2019 saw a large increase in these targeted ransomware attacks. The attackers are targeting large organizations, starting with extensive reconnaissance in the pursuit of large returns. However, McAfee states that despite all the new advanced attack techniques, the threat actors still rely on social engineering and human fault.

"*Analysis of these details shows threat actors are going after bigger fish, and they continue to use user execution and spear-phishing attachments in attacks*" (McAfee, 2019, p. 11). Check Point Research (CPR) agrees with McAfee and the NCSC that ransomware is in decline. They state that it might be because cryptomining is a more efficient alternative, however, "*It can also be related to the adoption of the 'boutique' ransomware attacks that only target specific organizations instead of wide global campaigns"* (CPR, 2019, p. 22). Boutiques ransomware attacks fit the same description as big game hunting. "*This new strategy allows threat actors to maximize their revenue, as a tailored attack against organizations' critical assets is a great tactic to ensure the ransom payments*" (CPR, 2019, p. 13). The targets for big game hunting which CPR describes are municipal "*IT infrastructures, hospitals seaports and airports newspapers and many other undisclosed institutions*" (CPR, 2019, p. 21). Big game hunting is ransomware adapted to ensure more profits. The infection stage has changed from spam to extensive reconnaissance on the organization. Symantec has noticed this change in ransomware attacks as well. They saw that ransomware is targeting enterprises instead of consumers.

"*From a tactical perspective, Accenture iDefense notes that ransomware attacks have risen as one of the key destructive tools used for financial gain, with attackers seeking extortion alongside sabotage and destruction*" (Accenture Security, 2019, p. 6-7).

Another threat which was mentioned by CrowdStrike was supply chain attacks. The NCSC also talks about the increase in successful attacks through third parties, they state it is becoming more attractive to gain access through third parties since more and more companies are aware of their digital weaknesses and therefore have increased their cyber security. McAfee has also seen an increase in supply chain attacks (sometimes described as third party attacks). In the first quarter of this year, a major software-update was compromised and contained malware. Symantec reported an increase in formjacking "*use of malicious JavaScript code to steal credit card details and other information from payment forms on the checkout web pages of eCommerce sites*" (Symantec, 2019, p. 14). This increase comes hand in hand with the increase in supply chain attacks, where malicious code is injected in legitimate software. In the case of formjacking, it was the result of the usage of compromised third party services such as chatbots. Accenture security has seen this rise in third party attacks as well. They state that attackers are trying to penetrate targeted networks through the networks of trusted partners. *"As ever, cybercriminals are persistent and inventive—if they can't get in one way, they will keep trying until they find another"* (Accenture Security, 2019, p. 6).

CrowdStrike also mentioned business email compromise also known as CEO fraud as an upcoming threat. This was also noticed by CrowdStrike Services. They stated that *"It often involves an actor sending an email from a spoofed or compromised account to the victim company's financial institution requesting a wire transfer. Once the transfer is sent, the payment details are intercepted by the criminals and changed. In other incidents, actors have targeted 401(k) accounts of employees or an institution's payroll system"* (CrowdStrike, 2019, p. 65). This attack is based upon social engineering, phishing and spear phishing, to gain access to a legitimate account of the targeted company. "*The fastest and most effective attacks continue to be those where attackers masquerade as legitimate users"* (CrowdStrike Services, 2018, p. 9).

CPR noticed that Botnets are on the rise as well, resulting in larger DDoS attacks. In 2018, the financial sector was targeted as well as the campaigns of US democrat candidates. DDoS attacks were used to disrupt the campaign website, denying voters key resources during periods of fundraising. "*From massive data breaches and crippling ransomware attacks to a meteoric rise in cryptojackers, there was no shortage in disruption caused to global organizations*" (CPT, 2019, p. 3). The NCSC and CrowdStrike also noticed the increase in DDoS and botnet attacks.

Manipulation of information and disinformation tactics are other threats which are mentioned by the NCSC and Accenture Security.

Finally, next to these threats, the NCSC also mentions phishing and physical operations to supplement hacking tools, a strategy often used by nation-states. "*Given the changing nature of geopolitical relationships, the greater the Dutch involvement in geopolitical conflicts, the greater the threat of disruption and sabotage will become*." (NCSC, 2019, p. 16).

Threat Actors

Nation-state actors have been indicted in 2018, however, according to CrowdStrike, they are showing no signs of stopping. According to CrowdStrike the main objective of the nation-state actors is collecting intelligence on foreign powers. CrowdStrike has identified targeted intrusion activities from multiple states around the whole world. "*In 2019, targeted intrusion adversaries will continue to conduct campaigns as part of their nation-state's national strategies"* (CrowdStrike, 2019 p. 72). CrowdStrike Services agree that nation-state attackers are one of the biggest threat actors. They state that nation-state attackers have incredible patience and capabilities. They mostly target high-value data in organizations. The NCSC agrees that the threat of the nation-state sponsored activities is growing. "*Today, digital threats are a permanent fixture and the scale of the threat posed by nation-state actors continues to grow. Countries such as China, Iran and Russia have offensive cyber programmes against the Netherlands"* (NCSC, 2019, p. 7). The NCSC also states that nation-states have started using cybercrime-as-a-service actors to outsource their execution of cyber attacks to third parties, providing them with even more digital knowledge and resources. *"Disruption and sabotage by nation-state actors have the greatest impact on national security*" (NCSC, 2019, p. 16). Nation-states are mentioned as threat actors by CPR as well. They have seen a trend emerge where nation-states do not use the cyberspace in secrecy anymore and operate relatively openly. As example they give Russian attacks against Ukraine, Black Energy which took down their power grid and NotPetya, which took down the entire country. "*The US and UK formally blamed Russia for the 2017 NotPetya ransomware attack that caused billions of dollars in damages worldwide"* (CPR, 2019, p. 11). Where the previous reports mostly attributed espionage to nation states, CPR takes it a step further. "*Alongside intelligence goals like espionage or surveillance campaigns, nation state* *cyber attacks exposed some new missions such as sabotage, financial gains and revenge*" (CPR, 2019, p. 17).

Next to nation-state actors, state-sponsored actors are a threat as well. Symantec for example, mentions the groups APT28 and APT29, cyber espionage groups which are attributed to Russia by the FBI and by Homeland Security. Accenture Security agrees that these actors should not be left out of the picture. Next to Accenture Security and the NCSC, McAfee and Symantec also discussed these actors.

CrowdStrike has detected a new trend in the eCrime ecosystem. The actors which CrowdStrike tracks, are increasingly working together. They are building alliances to achieve their goals. Next to working together, there is also an increase in the availability in buying access from other actors and TTPs-for-hire have become available as well. CrowdStrike Services noticed the same trends. The commodity malware market is increasing and threat actors are working together. "*Actors and tools that used to operate discretely now show evidence of working in coordination*" (CrowdStrike Services, 2018, p. 8). They add that eCrime actors are innovating and using more creative techniques to profit from their attacks. CrowdStrike Services calls the eCrime actors working together a "den of thieves". Symantec also sees a rise in attack groups as threat actors. *"Targeted attack actors continued to pose a significant threat to organizations during 2018, with new groups emerging and existing groups continuing to refine their tools and tactics"* (Symantec, 2019, p. 18). For example, Symantec states that most of the formjacking comes from a group named Magecars, which is believed to be multiple groups. CPR states that cybercriminals have matured. By starting to work together they pose a greater danger for organizations and have increased their ability to carry out high-profile attacks. *"Threat actors are merely adapting their techniques, sometimes in real time, offering an affiliate system to allow technically low-level criminals to get in on the lucrative form of attack"* (CPR, 2019, p. 5). Accenture Security compare the threat actors to chameleons, adapting and switching to new TTPs. "*We are seeing the emergence of new cybercrime operating models among high-profile threat groups. Relationships are forming among "secure syndicates" that closely collaborate and use the same tools— suggesting a major a change in how threat actors work together in the underground economy*" (Accenture Security, 2019, p. 4). These syndicates have stopped sharing their techniques with everyone but are sharing with smaller trusted groups.

Next to criminal groups, cyber criminals also known as eCriminals, remain an important threat actors as well. They are mentioned by CrowdStrike, Crowdstrike Services, the NCSC, McAfee, Check Point Security and Accenture Security *"Given that hacking tools are readily available and the efficiency of simple attack methods, a substantial threat is posed by a wide range of actors"* (NCSC, 2019, p. 18).

CrowdStrike also briefly mentions hacktivists. However, Accenture is seeing hacktivism being replaced by state-sponsored hacktivism. "*Nation-states are increasingly outsourcing malicious cyberoperations to cybercriminals to increase their capabilities and attain strategic goals—blurring lines between politically and financially motivated cyberthreat activities*" (Accenture Security, 2019).

Next to all the above-mentioned actors, the NCSC also touches upon scriptkiddies and cyber vandals.

Scope of the threat

"*Disruptions and systems failures will have a greater impact on society in the future due to the complete dependence on digitised processes and systems*" (NCSC, 2019, p. 5). More processes are becoming dependent on ICT. Next to becoming more dependent on ICT, according to the NCSC the Netherlands is becoming more dependent on providers of hardware and software. "*This dependence creates risks to national security*" (NCSC, 2019, p. 21). Another example of dependency of the Dutch society which they give is the telecom system. Many organizations were not aware of their dependence and were not prepared for disruption of this system. "*There is no plan B if the networks go down"* (NCSC, 2019, p. 22). Each threat has its own scope, its own level of disruption it can achieve. "*Each attack has an ultimate objective, such as theft of data or computing resources, and the attack typically requires multiple steps along the way to reach that objective*" (CrowdStrike, 2019, p. 19).

According to CrowdStrike cyber espionage can lead to intellectual property theft and can be the precursor of destructive attacks.

CrowdStrike also describes the consequences of big game hunting. They state it can lead to a large financial loss for the targeted company, or complete disruption of the business if the targeted company decides not to pay. One of the features of big game hunting is the deployment across the entire network of the organization, which can lead to complete disruption. The McAfee report also sets out the threat of big game hunting. It states that the targets can lose great amounts of money and even data or intellectual property if they are targeted. CPR gave an example of the consequences of big game hunting. "*In March, the SamSam ransomware struck the City of Atlanta in a big way by infecting and halting the operation of multiple city services for over a week. Services affected were the city's law courts that prevented court cases from proceeding, warrants being issued, and residents able to access the city fine online payment services*" (CPR, 2019, p. 5). The ransomware attacks which Symantec discussed were al targeted highly damaging attacks. This is in line with the disruptive threat of big game hunting as set out by the other reports. "*This interest in potentially disruptive attacks is also reflected in the number of groups known to use destructive malware, up by 25 percent in 2018*" (Symantec, 2019, p. 18). Accenture Security also mention that ransomware attacks are the most destructive tool used for financial gain. Attackers aim for extortion, sabotage and destruction. Some of the times, a ransomware attack may appear financially motivated. However, it may have other goals, therefore the payment of the ransom does not always guarantee in the restoration of the data. Due to the sale of access to corporate networks, ransomware has even become more dangerous. It has the potential to deploy on a corporate wide scale with the abilities to self-spread across the network.

CrowdStrike Services stressed the amount of disruption commodity malware attacks can have. These attacks can lead to compromised credentials, ransomware, theft of intellectual property and personal identifiable information, starting disruption campaigns or fraud through wire transfers. "*once access is gained, the organization is left completely exposed"* (CrowdStrike Services, 2018, p. 9).

The NCSC also reported about the level of disruption of DDoS attacks. While these attacks do not directly harm security, they do harm the trust in the digital infrastructure. *"Disruption and sabotage have the greatest impact on national security due to their potential to cause social disruption"* (NCSC, 2019, p.7).

CPR shows the scope of threat if a nation-state is involved. The Russian attacks against Ukraine has immense consequences. Black Energy had the ability to take down the entire power grid and NotPetya caused billions of dollars in damages worldwide through disruption.
Accenture Security mentions disruption trough disinformation due to digitization. "*The financial services industry—and, more specifically, high-frequency trading algorithms, which rely upon fast, text-driven sources of information—are likely to be targeted by large-scale disinformation efforts in the future"* (Accenture Security, 2019, p. 4).

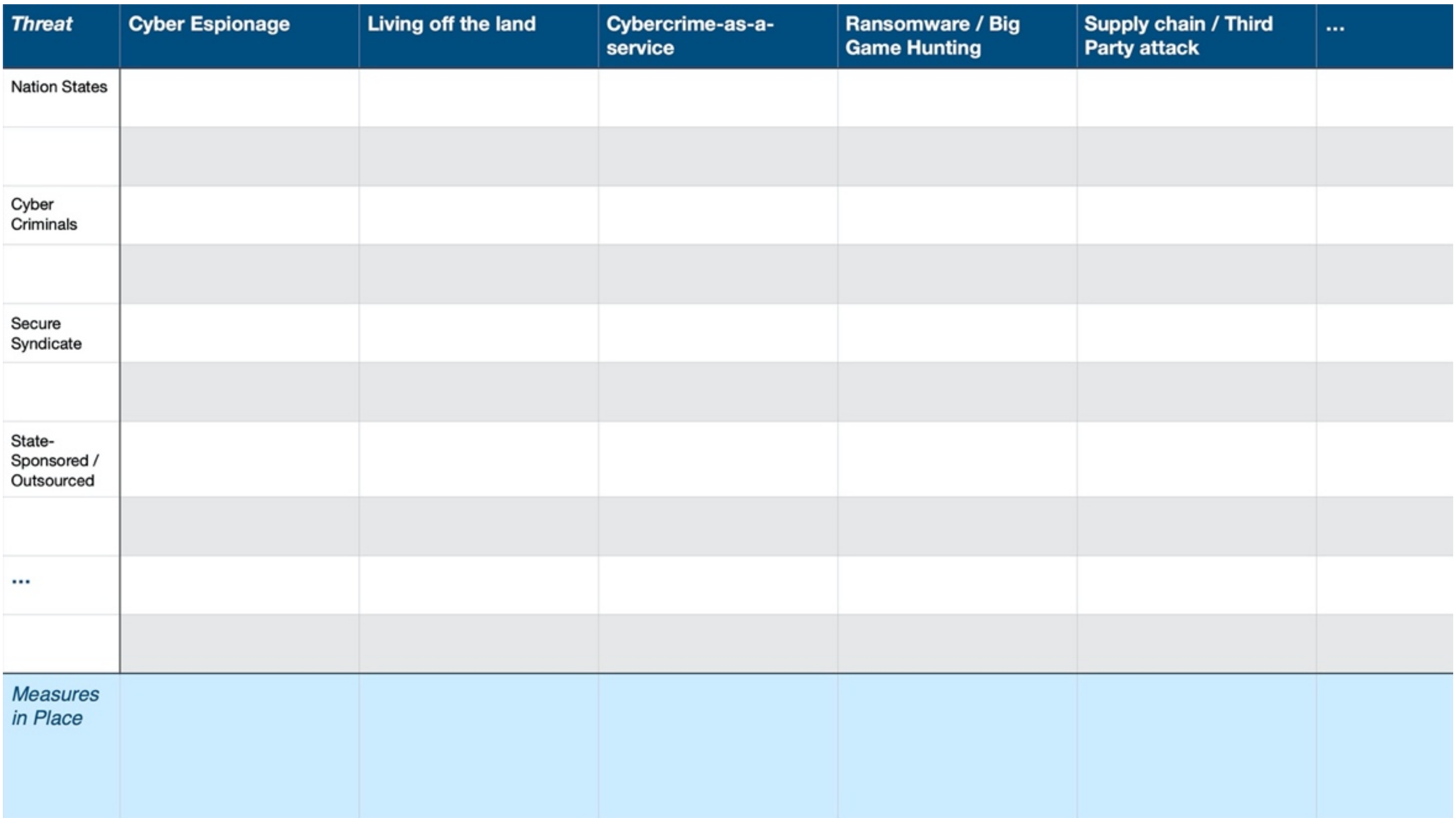
Break out time

The CrowdStrike Global Threat Report is one of the only reports which extensively describes the breakout time of cyber threats.

According to CrowdStrike, groups that were affiliated with the Chinese had a breakout time of four hours, while groups from China were faster. North Korea situated actors had a breakout time of around two hours, while Russian based actors were the fastest with a breakout time of fifteen minutes. The average breakout time that CrowdStrike observed was 4 hours and 37 minutes. "*Organizations can adjust their target response times to meet their individual needs, based in part on which adversaries types they are most likely to confront in their given business sector and regional focus*" (CrowdStrike, 2019, p. 15). *"An intruder only needs one hour and 58 minutes, on average, to jump from the machine initially compromised to begin moving laterally through the network*" (CrowdStrike Services, 2018, p. 4). While working on this content analysis, I noticed that only CrowdStrike and CrowdStrike Services indicate breakout times. Therefore, the breakout time is not taken into account as a category.

Results

Based on the data analyzed above, the following threat matrix was created. The matrix is created through quantitative analysis. The matrix will be used during the interviews with the selected companies, to determine their knowledge of cyber threats and threat actors and to determine what the measures in place are to prevent these threats, if there are any measures in place.



Threat	Cyber Espionage	Living off the land	Cybercrime-as-a-service	Ransomware / Big Game Hunting	Supply chain / Third Party attack	...
Nation States						
Cyber Criminals						
Secure Syndicate						
State-Sponsored / Outsourced						
...						
Measures in Place						

Cyber Threats

The threats that it includes had to be described in at least three of the seven analyzed reports. This reason this research has chosen that the threats need to be described in at least three of the seven analyzed reports is that the reports come from different companies with different threat perspectives. Therefore, it is highly unlikely that they all describe the same threats. If a threat is just mentioned in one or two of the reports, it is only perceived as a massive disruptive threat by 14% - 29% of the companies, not even one third of the analyzed reports. However, if three of the reports mention the threat, it is covered in 43% of the reports. If more than 40% of the reports mention the threat it cannot be left out of the matrix. The same rules apply to the threat actors. The threats that are selected will be defined and set out below.

Cyber espionage was mentioned by CrowdStrike, the NCSC and McAfee. It is defined as *"impairment of the confidentiality of information by means of the copying or removal of data by nation-state actors or nation-state-affiliated actors*" (NCSC, 2019, p. 49).

Living off the land was mentioned by CrowdStrike, the NCSC, Symantec and Accenture Security. It is defined as a "*tradecraft that uses legitimate tools already present on the target system to accomplish adversary objectives*" (CrowdStrike, 2019, p. 12).

Cybercrime-as-a-service was mentioned in different forms by CrowdStrike, CrowdStrike Services, the NCSC, Check Point Security and Accenture Security. Other terms used to indicate the same threat were crimeware distribution, commodity malware and affiliate systems. According to the NCSC (2019, p. 27) it "*enables actors with relatively limited capacity to execute cyber attacks". The* NCSC also (2019, p. 12) mentions that "*cyber attack capabilities can be easily obtained via commercial providers and via the substantial cyber criminal services sector."*

Big game hunting was mentioned by CrowdStrike, CrowdStrike Services, the NCSC, McAfee, Check Point Security and Symantec. Other terms to indicate the same threat were targeted ransomware and boutique ransomware attacks. It is defined by CrowdStrike (2019, p. 51) as *"eCrime operations using ransomware to target large organizations for a high return. Often, these sophisticated campaigns include well-tested reconnaissance, delivery and lateral-movement TTPs*". Check Point Research (2019, p. 13) adds that *"this new strategy allows threat actors to maximize their revenue, as a tailored attack against organizations' critical assets is a great tactic to ensure the ransom payments*".

Supply chain attacks were mentioned by CrowdStrike, the NCSC, McAfee and Accenture Security. It is also known as an attack through a third party. The definition is the following: *"Supply chain attacks, which exploit third-party services and software to compromise a final target, take many forms, including hijacking software updates and injecting malicious code into legitimate software"* (Symantec, 2019, p. 17).

Threat Actors

The same rules which were used to choose the right Cyber Threats for the matrix apply to the Threat Actors. So the actors should be described in at least three of the seven analyzed reports.

Nation-states were mentioned by CrowdStrike, Crowdstrike Services, the NCSC, McAfee, Check Point Security and Accenture Security. "*Nation states that execute cyber attacks on other nation states, organisation or individuals, primarily based on geopolitical motives. Their goal is to obtain strategically important data (espionage), exercise influence on public opinion or democratic processes (influencing) or to disrupt (disruption) or even destroy (sabotage) critical systems"* (NCSC, 2019, p. 50).

Cyber Criminals (eCriminal) were mentioned by CrowdStrike, Crowdstrike Services, the NCSC, McAfee, Check Point Security and Accenture Security.

The NCSC (2019, p. 47- 48) defines a criminal as "*An actor that conducts attacks based on economic or financial motives*." And Cyber crime as a *"Form of crime aimed at an ICT system or the information processed by this ICT system. There are various types of cyber crime: in a narrow sense, a type of crime targeting ICT (high-tech crime); a type of crime that is predominantly executed using ICT (cyber crime); in a broad sense, any form of crime that makes use of ICT in some way (digitised crime)."* Cyber Criminals are actors who conduct cyber crimes based on economic or financial motives.

Secure Syndicate is a term conceived by Accenture Security (2019, p. 4) "*We are seeing the emergence of new cybercrime operating models among high-profile threat groups. Relationships are forming among "secure syndicates" that closely collaborate and use the same tools— suggesting a major a change in how threat actors work together in the underground economy*". Next to Accenture Security, CrowdStrike, Crowdstrike Services, the NCSC, Check Point Security and Symantec also witnessed these relationships among threat groups. CrowdStrike Services came up with the term "Den of Thieves". There has been a significant rise in these high-profile threat groups. "*This interest in potentially disruptive attacks is also reflected in the number of groups known to use destructive malware, up by 25 percent in 2018*" (Symantec, 2019, p.18).

State sponsored actors were mentioned by the NCSC, McAfee, Symantec and Accenture Security. "*Nation-states are increasingly outsourcing malicious cyberoperations to cybercriminals to increase their capabilities and attain strategic goals—blurring lines between politically and financially motivated cyberthreat activities*" (Accenture Security, 2019, p. 5). Next to Accenture Security, the NCSC (2019, p.12), also talked about Nation-states outsourcing malicious cyberoperations. "*Nation states can 'outsource' the preparation for and execution of cyber attacks to third parties."*

Scope of the Threat

Defining the scope of these threats posed a more difficult task. The reports shied away from giving the specific consequences of the threats. These are some of the consequences these threats can have.

Cyber espionage can lead to intellectual property theft, duplication or manipulation of data and can be the precursor of destructive attacks (CrowdStrike, 2019).

Cybercrime-as-a-service can lead to ransomware, cryptomining, intellectual property and personal information theft. As CrowdStrike Services (2018, p. 4) stated "*once access is gained, the organization is left completely exposed."*

Big game hunting can lead to a large financial loss for the targeted company, or complete disruption of the business if the targeted company decides not to pay. "*The equation is simple though; the greater the potential damage, the higher the chance the ransom will be paid*" (CPR, 2019, p. 13). Check Point Security (2019) gives the example of the SamSam ransomware. This targeted ransomware halted the operation of multiple city services for over a week. Accenture Security (2019) even states that they are the most destructive tool used for financial gain.

Conclusion

The answer to the sub question "*What are massive disruptive cyber threats?"* is not straight forward. It depends on who the question is for. For example, in the interview with a government expert, he stated that small businesses often suffer insurmountable losses because hackers change the bank account number on their invoices. However, these small businesses will not have to fear big game hunting, since the cybercriminals know that there is too little to earn in relation to the effort of the attack.

Due to the different factors weighing into answering this sub question, this research focusses on larger companies. After the content analysis and the interview with the government expert it defines these threats as threats which disrupt the business continuity and bring the survival of the targeted or infected company in danger. These threats will be prioritized according to the level of disruption, starting with the threats that cause the least amount of disruption. These threats consist out of: 1) Living off the land by cyber criminals, secure syndicates and state sponsored actors. Since the actors use legitimate tools, this threat has the lowest level of disruption. 2) Supply Chain Attacks by secure syndicates, cyber criminals and state sponsored actors. This is a threat in which the actor gains access to your system, the level of disruption does not have to be immense. 3) Cybercrime-as-a-service offered by secure syndicates. Access to systems or other services are sold. Since this provides tools to almost all actors it is considered more disruptive than living off the land and supply chain attacks. 4) Cyber espionage by nation states or state sponsored actors. This can be highly disruptive. On the one hand in the form of leaked documents and secrets, on the other hand in the form of corporate espionage where your competitor gets ahead of you without investing in research and development. 5) Big Game Hunting by secure syndicates, cyber criminals and state sponsored actors. When you are targeted by big game hunting, your entire IT infrastructure is shut down. You cannot access your files unless you pay up or get them out of your system. This is one of the most disruptive threats that exist. 6) Destructive attacks by nation states or state sponsored actors. This is the most disruptive attack. Previous examples are NotPetya which caused 10 billion dollars in damages and Black Energy which shut down the Ukrainian power grid.

Check Point Security shows the scope of threat if a nation-state is involved. The Russian attacks against Ukraine had immense consequences. Black Energy had the ability to take down the entire power grid and NotPetya caused billions of dollars in damages worldwide through disruption. The NCSC (2019, p. 15) states in their report that "*Nation-state actors pose the biggest cyber threat to national security, and that threat continues to grow*". There are multiple disruptive cyber threats and threat actors, however, the most disruptive threat actors are nation-state (sponsored) actors.

Companies, Their Knowledge of the Cyber Threat Landscape and Their Cyber Resilience

To answer the second sub question *"How do companies see massive disruptive cyber threats and how are they prepared to deal with such threats?"* four expert interviews were conducted. The type of interview which was conducted was an elite/expert interview.

Due to the limited willingness of companies to participate in this research, four different types of organizations were interviewed. All the interviewees and interviewed organizations have been anonymized since all organizations gave detailed descriptions about the cyber resilience of their or other organizations.

The four types of organizations that have been interviewed are the following: 1) Government organization, 2) Large Company (+300 employees), 3) Cybersecurity firm and 4) Consultancy.

By conducting interviews in different types of organizations, I aspired to obtain a clear view on the cyber resilience of companies. The goal of these interviews was to find out what their view is on cyber threats, what the trends are in the cyber threat landscape and how their business continuity and disaster recovery plans work.

The interviews will focus on the cyber awareness and cyber resilience of companies. This is done by focusing on four different categories. Three of these categories are derived from the content analysis coding categories, since it aims to draw a conclusion on the same subject as the content analysis. The last category is the cyber resilience of the company. By analyzing the data obtained through these categories the second sub question will be answered.

Coding scheme

The following codes were used in the transcripts of the interviews:

- Cyber Threats (green)
  - What do they see as the biggest cyber threats?
  - What do they see as the biggest cyber threat for companies?
  - How do they see the threat landscape evolving?

- Threat Actors (yellow)
  - Who do they see as the biggest threat actors?
  - Who do they see as the biggest threat actor for companies?

- · Scope of the threat (blue)
  - What kind of impact do they expect cyber threats to have?
  - How do they perceive the threat matrix?

- Cyber resiliency (red)

- What are the biggest weaknesses of companies?
- How is their cyber security arranged?
- What are their response strategies?
- Do they have business continuity / disaster recovery models in place?
- What should the cyber security of a company look like?
- What kind of measures should a company take to become cyber resilient?

Cyber threats, threat actors, scope of the threat and cyber resiliency are the indicators that are used. The indicators need to be discussed to be highlighted. Answers given by the interviewee have to be specifically pointing to that indicator for it to be highlighted. A simple mention of the indicator is not enough to be highlighted. The highlighted transcripts are to be found in the annex. The following section of this chapter will go into the results of the interviews. It will start by discussing the results of the first three indicators which were also used in the content analysis, after which it will also compare the results with those of the content analysis. Finally, it will discuss the cyber resilience of the company. These results will be taken into the next chapter where they will be analyzed using business continuity and data recovery models.

Results

Cyber Threats

In all the interviews, cyber threats were discussed extensively. On the basis of the knowledge of the interviewees and by showing them the threat matrix. The government organization was interviewed through the phone, so the analysis of the threat matrix was left out of the interview. The government expert mentioned the following threats. Cybercrime-as-a-service has been going on for a long time, it has democratized the ability to carry out cyber attacks. According to him, you do not need any expertise anymore. Big companies are becoming more interesting, since ransomware distributers are beginning to focus on targeted attacks, they infiltrate the company and find out how much they can ask. He stated that if your security is good enough, the attackers will try to get in through your third parties or supply chain. "*From a defensive view, third parties are a weak point*".

The consultancy expert gave his view on this subject as well. He stated that worms which are able to propagate extremely fast are one of the biggest threats. As an example, he gave the NotPetya and the Conficker viruses. He stated that Black Swan events exist and have the potential to do a lot of damage since almost everyone uses the same operating system with the same vulnerabilities. As well as the government expert, he explained that the average amount of ransomware is down, but that the criminals have changed their methods into more targeted attacks. They get into people's system and put the ransomware where it is the most painful for the business. He also agreed that the tools available are increasing through cybercrime-as-a-service. He specifically mentioned ransomware-as-a-service, but stated that high-end attacks will become much more targeted. Next to these threats he also mentioned intellectual property theft and the theft of personal information, he saw the IoT as an upcoming threat and saw cyberwarfare as the future of warfare.

The expert of the cyber security firm explained that they do see disruptive attacks happening. They response to about 100 to 150 incidents a year and a few of them are disruptive attacks. According to him the biggest threats for companies were targeted ransomware attacks and disruptive attacks from state to state under which companies suffer, for example NotPetya. The targeted ransomware has evolved to infiltrate the company get to know the network, infiltrate the back-up and put the company down. He did not think that the threat landscape changes that frequently. He explained that ransomware is a business model, criminals are busy earning money, not inventing new techniques. "*I think ransomware is going to remain lucrative and profitable for criminals for the time being and I don't think they will abandon it.*" He also saw DDoS attacks as a threat, however the company extortion through the threat of DDoS had become less. His views agree with the government expert that cybercrime-as-a-service is nothing new and has been happening for the last years. He also mentioned the threat of states who steal information and disrupt along with the example of the emails of the Democratic National Committee which were leaked by Russia. The IoT was not mature enough to be seen as a threat. While living off the land and third party attacks were more of a method of operation to get in and attack than a threat according to him. "*If we talk about threats, we talk about information theft, disruption and extortion.*"

The IT director of the company that was interviewed had a different view on disruptive cyber threats. He had less knowledge on the cyber threat scape, but showed knowledge and understanding about the threats the company faced. One of the threats he had faced at a previous employer was a hacker who disrupted their websites. Next to that, he stated that viruses were a big threat for them, data corruption and social engineering. The previous company he worked for, was a retail organization. He explained that if you dressed up nicely, you could smooth talk your way in and get access to a workspace. He was less familiar with living off the land and third party attacks, however, ransomware was known and perceived as a threat.

Concluding, cyber espionage was mentioned as a threat in the form of intellectual property theft carried out by states by the consultancy and the cyber security firm. Living off the land was an unfamiliar term for most of the interviewees knew. Where the government expert define the supply chain as a weakness, the expert from the cyber security firm defined it as a method of operation instead of a threat. Cyber-crime-as-service was defined by the government and cyber security firm experts as a threat which has been going on for quite some time. All the interviewees agreed that big game hunting is a threat which is gaining momentum and can be disruptive for companies.

Threat Actors

The government expert explained that at this time, there are motivated actors with the capabilities to disrupt. Through cybercrime-as-a-service, you need to know less and are still able to carry out an attack. Next to this, he also stated that states make use of these services. According to him they prefer simple attacks, where the targeted company thinks it is a unsophisticated attacker, so that they will not be recognized.

The expert at the consultancy explained the threat actors have changed. Where fifteen years ago they were just pranksters, now they are changing into professional businesses. He gave the example of a bank who was targeted by ransomware. The attackers offered additional services upon giving the decryption key, they would decrypt the files and upgrade their security. *"They are becoming much more sophisticated in terms of how they hurt the business and how they can extract the greatest ransoms and extortions".* Next to the professionalization of the criminal actors, the nation states are a big threat as well. The lines between nation states attackers and some hacking groups are becoming blurred, more states are using hacking groups to do their dirty work. Some nations are also starting to use hacking as a revenue source, North Korea is even putting the smartest kids in hacking schools. "*Any country that is heavily sanctioned is going to probably use hacking as a revenue source*." Finally, he mentioned that hacktivists have gone down in importance.

According to the expert at the cyber security firm there are two main groups of threat actors, criminals and states. Everybody needs to keep the criminals in mind, they will keep using techniques that exist and are available. Crime groups are nothing new, according to him there were already groups of Russians carrying out hacks more than 10 years ago. At his firm, they see criminals and criminal groups as one type of actors. "*The goal for criminals is about earning money and I think that ransomware will be the best way for the time being".* State actors are the actors who are capable of disruptive attacks. There are state sponsored groups, who do not officially belong to the government but do carry out attacks for them, his firm sees states and state-sponsored groups as one kind of actor. His views contested the views of the government expert. According to him states do not use cybercrime-as-a-service, they make their own malware so they can completely control it. However, you see them using open source tools more often. He also mentioned that states have started to use hacking as a revenue source. Next to states and criminals he identified scriptkiddies and hacktivists as actors which are not a big threat, but should not be underestimated. Finally, he identified malicious inside actors as a serious threat, since they know your company from the inside. Criminals do not disrupt, mostly states.

The interviewed company identified cybercriminals and states as the main threat actors, however, they only perceived cybercriminals as a serious threat for themselves, since they do not perform state or critical infrastructure related activities.

Concluding, the interviewees defined states along with state sponsored actors and cyber criminals, as well as cyber criminals working together as the most prominent threat actors. However, they added that through cybercrime-as-a-service everyone is capable of carrying out a cyber attack.

Scope of the threat

According to the government expert, disruptive attacks are imaginable situations. Cybercriminals will mostly try to earn money, where the disruption is a side effect. However, for small companies, a hack by a cybercriminal could already be enough to bankrupt them. Attacks by states, for example sabotage, often have disruption as a goal and are therefore able to take down bigger companies.

The expert at the consultancy added legal ramifications of cyber threats as a disruptive factor. He gave the example of Diginotar, the company went bankrupt after multiple lawsuits and after the people lost their trust in them. Next to legal ramifications, he states that cyber attacks which can disrupt the computers and cause them to stop working would often suffice to bankrupt a company.

The interviewee at the cyber security firm states that only a small percentage of the incidents they respond is disruptive. Targeted ransomware is not a destructive attack, but most definitely disruptive for almost all companies. It used to be targeted on consumers, until criminals figured out that attacking companies was a lot more profitable. For small businesses targeted ransomware is less of a threat, since the criminals know there is nothing to gain. "*As criminal whose goal is to earn money, it is senseless to not give you your data back, because the story will spread, nobody will be sure if they get their data and nobody will pay."* He stated that criminals are the most dangerous actors for companies, unless you are the target of state actors.

The IT director of the company said there was only a small chance of a cyberattack, however he had experienced a couple. He emphasized the importance of keeping good back-ups.

All interviewees agreed on the scope of the threats which were intellectual property theft, financial loss or complete disruption of the business.

Threat Reports vs. Expert Interviews

In the interviews, the interviewees first had to mention what they perceived to be the biggest threats and threat actors. Afterwards their answers were compared to the results from the reports and the differences were discussed.

The threat reports defined cyber espionage, living off the land, cybercrime-as-a-service, big game hunting and supply chain attacks as the biggest threats. The results which came out of the interviews were significantly different. Cyber espionage was also mentioned as a threat in the form of intellectual property theft carried out by states by the consultancy and the cyber security firm. Living off the land was a term not many of the interviewees knew. The expert from the cyber security firm was familiar with the threat, however, he defined it as a method of operation not a threat. He defined supply chain attacks as a method of operation as well. However, the government expert did define the supply chain as a weakness. Cyber-crime-as-service was defined by the reports as a threat which was gaining momentum. The government and cyber security firm experts did not agree, they stated that this has been going on for quite some time. The government expert mentioned that states also make use of this new service, where the cyber security firm expert said this was not the case and the government does not trust other parties with their cyber attacks. All the interviewees agreed that big game hunting is a threat which is gaining momentum and can be disruptive for companies. The expert from the consultancy said the following about ransom distributors *"They are becoming much more sophisticated in terms of how they hurt the business and how they can extract the greatest ransoms and extortions".* Next to the threats which were chosen from the reports, the interviewees mentioned disruptive attacks from states, DDoS attacks and worms. However, to quote the expert from cyber security firm about the most significant threats "*If we talk about threats, we talk about information theft, disruption and extortion."*

The threat actors which came out of the reports were nation-states, cyber criminals, secure syndicates and state sponsored actors. All the interviewees agreed that those are the most prominent threat actors. The government expert added that everyone is capable of executing a cyber attack through cybercrime-as-a-service. The expert from the cyber security firm contested the threat actors set out by the reports. He stated that states and criminals are the most important actors, however, he did not distinguish state sponsored actors and states and he did not make a distinction between cybercriminals and cybercriminal groups as well.

The scope of the threats which were set out by the reports were intellectual property theft, financial loss or complete disruption of the business. The expert from the consultancy added legal ramifications and loss of trust. The expert of the cyber security firm states that mostly states carry out disruptive attacks, since criminals just want to earn money. *"As criminal whose goal is to earn money, it is senseless to not give you your data back, because the story will spread, nobody will be sure if they get their data and nobody will pay".* However, attacks by cybercriminals can be destructive for smaller companies.

After carrying out the interviews with the cyber security experts the answer to the sub question "*What are massive disruptive cyber threats?"* should be revisited. After the content analysis and the interviews with the cyber security experts this research defines these threats as threats which disrupt the business continuity and bring the survival of the targeted or infected company in danger. These threats will be prioritized according to the level of disruption, starting with the threats that cause the least amount of disruption. These threats consist out of: 1) Cyber espionage by state actors. 2) Cybercrime-as-a-service offered by cybercriminals. 3) Big Game Hunting by cyber criminals and state actors. 4) Destructive attacks by state actors.

Cyber resiliency

According to the government expert the companies are not resilient enough. *"Companies are having difficulties with the organization of resilience to protect themselves to these threats."* While large companies are becoming more aware, most companies still do not allocate enough budget and are still struggling to get the basics right, for example patch management and two factor authentication. Those simple measures can help resist cyber threats. Next to these simple measures, he also stated that while systems are getting more interconnected and dependent on each other, companies do not think about the consequences and vulnerabilities it brings.

The expert from the consultancy agrees with the government expert that largest weakness of companies is getting the basics right. "*The basics you know, so this is a common complaint. Almost every company doesn't get the basics right but getting the basics right is actually really hard. It seems simple because we call it basics, but actually doing this is a challenge for most companies."*

Another weakness he encountered during his work was that companies do not test their backups. He mentioned most companies have backups, for which they pay. However, in the end they do not trust them, since most of the time they have not tested them to see if they can do a full recovery. So when the moment comes, they are afraid to rely on their backups.

Next to the backups, he stated that companies do not know their landscape and therefore have a lot of blind spots. They do not have an inventory lists of their business-critical assets and a list of all their software. According to the consultancy expert there is a lack of governance.

In terms of business continuity planning, he advises companies to 1) identify their business-critical list, 2) to have recovery point objectives (RPO) and recovery time objectives (RTO), these are the length of your backups and how fast you would need them. 3) Create roles, responsibilities and accountabilities. Set up a governance plan and a communication run book. 4) The final step is to test the plans.

In the terms of disaster recovery planning, he stated that it is critical to start with backups and the RPO and RTO. Next to these two it is very important to test them in full recovery. *"You have to test them, because if you don't have trust in the system, you're just throwing money away every month."*

According to the expert at the cyber security firm, companies do not take into account black swan attacks. Next to that he stated that *"A lot of companies have deferred maintenance, which is expensive to fix. So at a lot of companies, there has to happen a lot to get on a level to protect themselves against these things (Black Swans)."*

The cyber security firm sees security as prevention, detection and response.
He stated that the basics prevention measures are the most important. Patch management, awareness of your employees, make backups, test those backups and implement measures that your backups cannot be tempered with, since that is what criminals do. You need to have your entire IT infrastructure under control. Detection does not happen enough according to him. Businesses need to know what is happening on their network, keep an eye on who logs in at what time and test their network security. It is important to log the right things so there is forensic material to investigate. Finally, companies need to create crisis plans and practice them yearly. *"So, it is about what do I protect against whom. Try to prevent using technical, historical and human measures and try to detect what slips through as fast as possible to react adequately."*

When working on data recovery, it is important to find out what systems have been compromised and where the attacker has been. You do not interrupt the attacker until you know what he is up to. Because when he knows he is found, you do not know what he is going to do. According to the expert, you see more and more business continuity and data recovery plans, however most of the times cyber security is left out. He gave the following metaphor regarding prevention: *"It is like if you protect your house against burglary. Then you have to take measures, perhaps you lock your door, but depending on who you protect yourself against. For example, if there is a lot of organized crime, then you may not only have your door locked, but for example you see that in Malaysia or in India, they have very large gates stand around a house. So, you have to start protecting yourself better, but if you want to protect yourself against James Bond, that's not enough. Then you have to seal all your windows with alarm things and stuff. The same applies here, the measures are actually the same. They just run up a bit, you have to do better. So if you want to protect yourself against an occasional thief, it really doesn't matter if you occasionally don't lock your door. That occasional thief doesn't really come every day. But if you protect yourself against James Bond, it is important because James Bond is lurking in the bushes. And if you forget it for once, he's inside. That is how we look at it, so actually all those measures are Prevention, Detection, Response."*

According to him, when you start at zero, it makes no sense to think about high-end threat actors. You first need to get your basics right.

The interview with the IT director of the company focused on the cyber resilience at the company where he is employed. The director said that the cyber awareness is growing at the company, the budget is available and management is willing to invest. "*Cyber is important at [name of company] we have decided to first make a framework in which we map all our exposures and what we need to protect them.*" They are protected with antivirus software, their depots and offices are well secured, you need a device to get to the workspace, you need to log in an extra time to get into the business applications, the network is controlled centrally, the network traffic is scanned and the customer portals are scanned as well. All their systems are backed up in a data center which is redundant. So if one server burns down, they have a backup which mirrors the data.

There were other points which required improvement. The cyber awareness among employees is too low and the laptops are not well protected. At the depots they still have passwords laying around sometimes. However, they have hired a company which is going to start a cyber awareness campaign and help them increase the security at the workspaces. Next to this, the plans were also there to start yearly penetration tests.

There is a business continuity plan, however it does not take into account cyber security. There is no formalized response strategy, but the director has a plan in mind. Firstly, he would call the IT staff together, do an impact analysis and look how to minimize damages. Secondly, he would close off the targeted system and investigate where the attacker is, isolate him and kick him off the network. In the meanwhile, they would look at the kind of business impact the attack has and see what is necessary to continue business. If they would to be targeted, their business can continue without a system at least for a day. The longer it takes, the more of a problem it becomes, IT is very important for them, but with good protocols they can run their depots without a system. He stated: *"Our company can work fairly without IT infrastructure."*

The Cyber Resilience of the Interviewed Company According to the Experts

Firstly, the cyber resilience requirements given by the government expert, the expert from the consultancy and the expert from the cyber security firm will be set out. Afterwards, the measures in place by the company will be analyzed through the scope of the requirements set out beforehand.

All the experts agree that getting the basics right is the most important factor of cyber resilience. The requirements will be set out along the model of the cyber security firm, as prevention, detection and response.

Prevention will be achieved in seven steps: 1) Identify the business-critical list, 2) patch management, 3) employee awareness. 4) have recovery point objectives (RPO) and recovery time objectives (RTO), 5) create roles, responsibilities and accountabilities, set up a governance plan and a communication run books 6) set up a crisis plan and 7) test all the plans and backups.

Detection is more difficult, it comes down to keeping you IT infrastructure under control. Businesses need to know what is happening on their network, keep an eye on who logs in at what time and test their network security, that way the chance an intruder is found is more likely.

Finally, response. With response it is important to find out what systems have been compromised and where the attacker has been. When you figure that out, you get him out of your system as fast as possible and try to close the opening through which he entered.

The interviewed company was working to improve their prevention. They were busy making a framework to identify their exposure and business critical assets. Patch management did not come up in the interview. They have hired a company to improve employee awareness. All their systems are backed up in a datacenter which is redundant. However, there is no governance plan or crisis plan in place. Nevertheless, the IT director has an unformalized plan.

The company has detection measures in place, they control the network centrally, they scan the network traffic and the customer portals as well.

They had no formalized response plan in place. However, the plan he had in mind did match what the expert advised. The company would do an impact analysis and try to minimize damages. Then they would try to isolate the attacker and kick him off the network. The company is able to continue their business for a limited time without a system.

Conclusion

To conclude this chapter, the sub question *"How do companies see massive disruptive cyber threats and how are they prepared to deal with such threats?"* will be answered.

When comparing the results of the interviews with the content analysis, it is clear that the reports name more threats and make more distinctions between actors. The threat matrix provided an overview of almost all the threats and threat actors which the interviewees named. However, some of the threats mentioned, could be better described as a delivery method to an actual cyber threat than the threat itself. The threat matrix also mentioned four different groups of actors, where the interviewees mostly saw states and state-sponsored groups as the same threat actors and crime groups (secure syndicates) and cybercriminals as the same threat actors as well.

After analyzing the interviews at the hand of the first three categories, namely; cyber threats, threat actors and the scope of the threat, it can be concluded that companies see massive disruptive cyber threats as threats which disrupt the business continuity and bring the survival of the targeted or infected company in danger with a realistic chance of happening. At the cyber security firm, they see several of these threats every year and the government expert referred to the report which stated that disruption of society by cyber threats looms ahead. After discussing multiple threats and threat actors, the following are the disruptive cyber threats which companies see: 1) Cyber espionage by state actors. 2) Cybercrime-as-a-service offered by cybercriminals. 3) Big Game Hunting by cyber criminals and state actors. 4) Destructive attacks by state actors.

In the interviews with the experts it came forward that companies are not prepared for these threats. Firstly, the expert from the government said that companies are having difficulties with the organization of resilience. Secondly, the expert from the consultancy said that almost every company does not get the basics right. Finally, the expert from the cyber security firm said that most companies do not even take these threats into account.

The company that was interviewed was cyber resilient enough for their probable threat actor. The IT director had a clear vision on how to protect the company and was busy improving their defenses as well. Their prevention was almost completely in order according to the standards set out by the experts. They had detection measures in place. However, despite that the IT director has an idea what to do they did not have a response plan in place. Nevertheless, as set out by the expert of the cyber security firm: "*If you protect yourself against scriptkiddies, you have to protect yourself for 70%, if you protect yourself against criminals it has to be 80% and if you protect yourself against states, you have to be as close as possible to the 100%.*" The interviewed company is protecting themselves from criminals and not Jams Bond. Not everything has to be perfect, but the basics have to be in place. With all the measures in place and the actions taken to improve their prevention measures, this company is cyber resilient enough for their probable threat actor. However, if they would be targeted by a massive disruptive cyber threat, their measures in place would not suffice.

Cyber Resilience

This chapter will answer the third sub question: *"What does business continuity and business survival mean for the researched companies and what should a relevant business continuity and disaster recovery plan look like?"* It will aim to answer this question by firstly analyzing the answers given by the interviewed company and secondly by comparing the requirements to achieve cyber resilience given by the government expert, the expert from the consultancy and the expert from the cyber security firm with an existing business continuity and disaster recovery plan.

The interviewed company is a logistics service provider in the supply chain of retail businesses. For them, business continuity and business survival is defined by that they can still provide their services to their clients. In the interviews with the experts came forward that one of the most important things for companies regarding business continuity is to keep the business-critical assets of the company running. So for the researched companies business continuity and business survival means that they can continue providing services and keep access to their business-critical assets.

The experts agreed that most companies do have business continuity plans. However, in most of these plans, cyber security is not taken into account. When interviewing the IT director of company X this came forward as well. They did have a business continuity plan in place which focused on IT, but it did not take cyber security into account. However, as the expert of the cyber security firm stated, you need to have a completely different plan for when the systems go down because of a cyber attack, then when your system goes down because someone tripped over a cable. In normal business continuity plans the attacker is not taken into account. The findings regarding cyber resiliency which came out of the interviews are set out in the table 2.

Prevention	Detection	Response
Identify the business-critical list	Analyze network traffic	Find the compromised systems
Patch management	Test network security	Find out how the attacker got in and in what systems he is
Employee awareness	User activity management	Get the attacker out of the system
RPO & RTO's in place		Close the openings through which he came in, make sure he has not left a backdoor so that he cannot come back
Set up a governance plan and a communication run books		Clean the compromised systems and restore corrupted files from backups
Set up a crisis plan		Make a report to the responsible government authorities
Test all the plans and backups		

Table 2.

These measures all are basic cyber security measures. All the experts agree that getting the basic cyber security measures right is the most important factor of cyber resilience. The better you implement these measures, the smaller the chance is an attacker or a massive disruptive cyber threat for that matter will be able to compromise your system. As the expert of the cyber security firm stated: *"The more you have to protect your company against high-end threat groups, the better you should implement them (The prevention, detection and response measures). Patch management is a good example, if you only need to protect yourself against script kiddies then you should do patch management well, but if you have to protect yourself against the Russians you really have to do it perfectly. Then you really can't afford mistakes because those Russians are able to take advantage of that one patch that you forgot."* So to answer the question what a relevant business continuity and disaster recovery plan should look like, it should include the measures as set out in the table above. With these measures, this chapter will seek to build upon the IBCDRP of Sahebjamniaa et al. (2015) to create a cyber resilient business continuity and disaster recovery plan.

According to Sahebjamniaa et al. (2015) businesses are encountering more disruptions. They argue that companies need a proactive approach with a decision support framework to help them protect themselves from these disruptions. Figure 3. (p.10) illustrates the proposed IBCDRP model of Sahebjamniaa et al. (2015). This model addresses the problems on three different levels: Strategic, Tactical and Operational.

At the Strategic level, the business is explored, the goal of the framework for the specific company is formed, the business operations are analyzed, the business-critical assets (in this framework, the critical operations (CO)) are listed and the company's resources are identified. Next to the business, the chance of it happening and the kind of disruptive events which could occur will be examined as well.

At the Tactical level, the CO's are analyzed. The MBCO and MTPD of the CO's are defined. Since every disruptive event will reduce the resources available for the company, the remainder of resources must be allocated to guarantee business continuity, to restore the disrupted operations and to recover the potentially lost data. *"The optimal resource allocation not only ensures resuming and restoring of disrupted operations, but also makes a trade-off between continuity and recovery plans"* (Sahebjamniaa et al. 2015, p. 261).

The Operational level is about testing, "*selected BC and DR plans are worthless unless they are rehearsed"* (Sahebjamniaa et al. 2015, p. 264). This model proposes to test the effectiveness of the plans with simulated hypothetical disruptive events. If these plans are in accordance with the MBCO and the MTPD the framework will be validated, if not changes are to be made at the tactical level. The RTO should be less than or equal to the MTPD and the RPO should be more than or equal to the MBCO. *"To reach an integrated BC/DR planning, decision- makers must consider a number of options to effectively allocate the available resources for continuity and recovery purposes of the organization"* (Sahebjamniaa et al. 2015, p. 265)

This model focusses on disruptive events, however, it has not been designed in the light of a disruptive cyber event. Therefore, the model needs to be upgraded to in relation to cyber resilience. The model focusses on the pre-disaster timeframe, in regard to massive disruptive cyber threats it is also important to implement measures for during and after the disaster. To upgrade this model the findings regarding cyber resiliency from the interview will be added. The upgraded model is to be found on the next page. The strategic, tactical and operational can be seen as part of the prevention of a massive disruptive cyber threat. The model already contained most of the measures set out in the table. It suggests identifying the business-critical list (critical-operations), it states that the RPO and RTO' need to be determined, it advises to set up governance and crisis plans and to test all these plans. The only thing missing in the prevention section was threat prevention. In the model on the next page this is added and consists out of patch management and increasing employee awareness.

The next sections added is detection. Detection was missing from the framework and is crucial to minimize the damage of massive disruptive cyber threats. Detection happens mid-disaster, meaning the moment the detection happens. Detection happens on the operational level and consists out of analyzing network traffic, testing network security and managing the user activity.

The last section added is response. Response happens post-disaster, meaning the moment the attacker is detected and the disruption has happened. Response happens on the operational level as well. It consists out of finding the compromised system, finding the attacker, figuring out how the attacker got into your system, closing the openings the attacker used to get in, making sure there are no backdoors left, cleaning the compromised system, reporting the incident to the responsible government agency and restoring the corrupted files from backups.

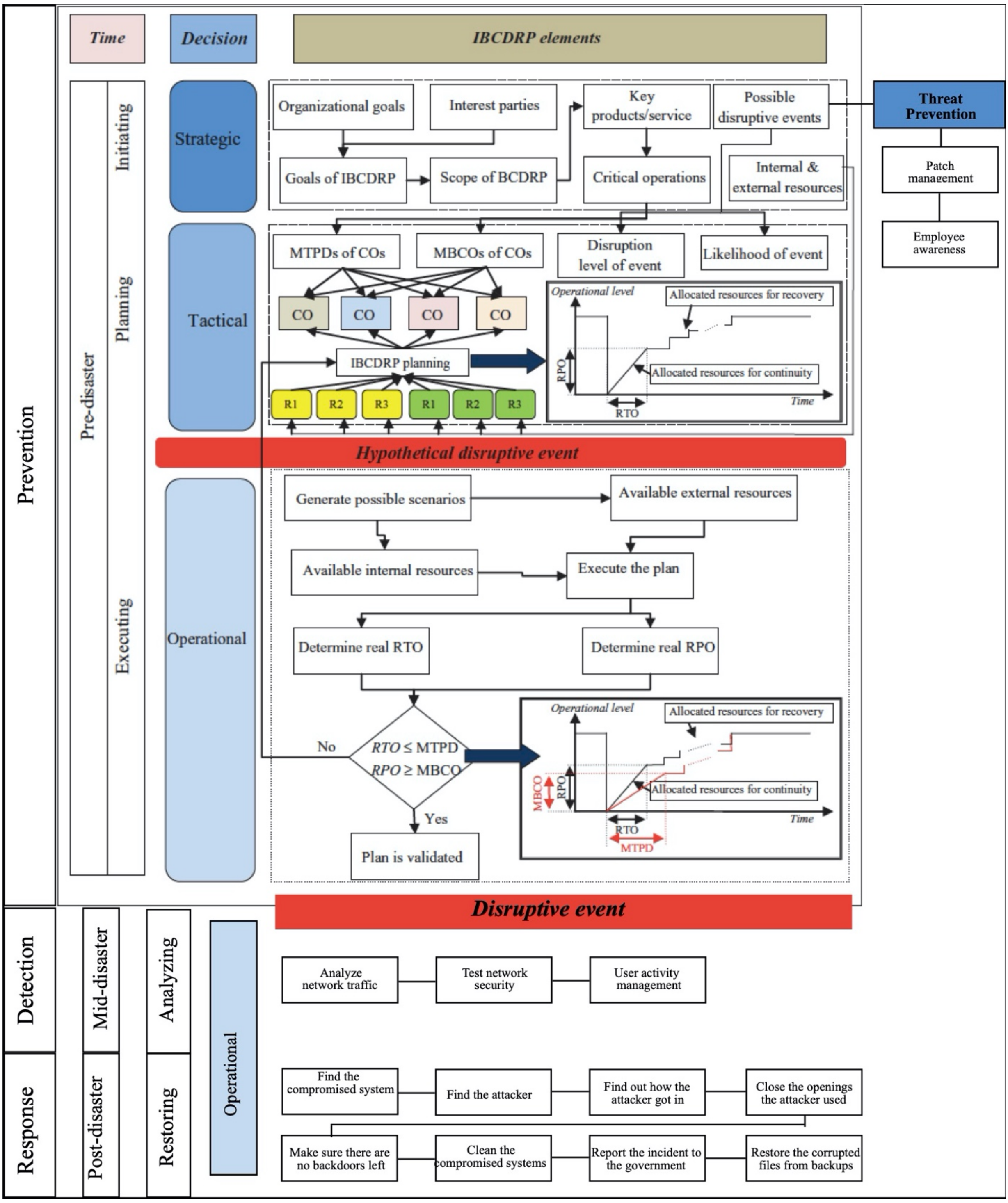


Figure 4. The Integrated Business Continuity & Disaster Recovery Planning upgraded to achieve Cyber Resilience (IBCDRPCR)

Concluding, to answer the third sub question: *"What does business continuity and business survival mean for the researched companies and what should a relevant business continuity and disaster recovery plan look like?"* this chapter analyzed the findings regarding cyber resiliency which came out of the interviews and set it out in a table. Using these findings, the IBCDRP framework by Sahebjamniaa et al. (2015) was upgraded to the model above. Thus, business continuity and business survival means that the businesses can continue providing services and keep access to their business-critical assets. A relevant business continuity and disaster recovery plan which can help the companies achieve this is set out on the previous page.

Conclusion

This research paper set out to answer the research question: "*To what extent do companies take into account massive disruptive cyber threats in regard to business continuity and business survival, and how can companies prepare themselves to make them more cyber resilient?*" To answer this research question, three sub questions were set out. 1) *What are massive disruptive cyber threats?* 2) *How do companies see massive disruptive cyber threats and how are they prepared to deal with such threats?* 3) *What does business continuity and business survival mean for the researched companies and what should a relevant business continuity and disaster recovery plan look like?*

To answer the sub question "*What are massive disruptive cyber threats?"* a content analysis was carried out. Seven cyber threats reports from different organizations were analyzed to find out what the biggest cyber threats were, the most capable threat actors and the scope of these threats.

Due to the different factors weighing into answering this sub question, this research focusses on larger companies. After the content analysis it defines these threats as threats which disrupt the business continuity and bring the survival of the targeted or infected company in danger. These threats consist out of (prioritized by the level of disruption): 1) Living off the land by cyber criminals, secure syndicates and state sponsored actors. 2) Supply Chain Attacks by secure syndicates, cyber criminals and state sponsored actors. 3) Cybercrime-as-a-service offered by secure syndicates. 4) Cyber espionage by nation states or state sponsored actors. 5) Big Game Hunting by secure syndicates, cyber criminals and state sponsored actors. 6) Destructive attacks by nation states or state sponsored actors.

"*Nation-state actors pose the biggest cyber threat to national security, and that threat continues to grow*" (NCSC, 2019, p. 15). There are multiple disruptive cyber threats and threat actors, however, the most disruptive threat actors are nation-state (sponsored) actors.

The sub question *"How do companies see massive disruptive cyber threats and how are they prepared to deal with such threats?"* was answered by conducting several interviews. The first thing that stood out was that when comparing the results of the interviews with the content analysis, the reports name more threats and make more distinctions between actors. Several of the threats which were set out in the threat matrix, were described as methods of operations instead of threats by the interviewees. Next to that, the interviewees saw two groups of actors instead of four. They saw states and state-sponsored groups as the same threat actors and crime groups (secure syndicates) and cybercriminals as the same threat actors as well.

It can be concluded that companies see massive disruptive cyber threats as threats which disrupt the business continuity and bring the survival of the targeted or infected company in danger with a realistic chance of happening. At the cyber security firm, they see several of these threats every year and the government expert referred to the report which stated that disruption of society by cyber threats looms ahead. After discussing multiple threats and threat actors, the following are the disruptive cyber threats which companies see: 1) Cyber espionage by state actors. 2) Cybercrime-as-a-service offered by cybercriminals. 3) Big Game Hunting by cyber criminals and state actors. 4) Destructive attacks by state actors.

In the interviews with the experts it came forward that companies are not prepared for these threats. The company that was interviewed was cyber resilient enough for their probable threat actor. However, if they would be targeted by a massive disruptive cyber threat, their measures in place would not suffice.

To answer the final sub question: *"What does business continuity and business survival mean for the researched companies and what should a relevant business continuity and disaster recovery plan look like?"* the findings regarding cyber resiliency and business continuity which came out of the interviews were analyzed. For the interviewed companies business continuity and business survival means that the businesses can continue providing services and keep access to their business-critical assets. The findings regarding cyber resiliency were set out in a table, which was used to upgrade the IBCDRP model by Sahebjamniaa et al. (2015) into a relevant business continuity and disaster recovery plan which can help the companies achieve more cyber resiliency the IBCDRPCR (figure 1 in the chapter: Cyber Resilience).

Starting this research, my hypothesis on the question "*To what extent do companies take into account massive disruptive cyber threats in regard to business continuity and business survival, and how can companies prepare themselves to make them more cyber resilient?*" was that massive disruptive cyber threats are not taken into account, companies underestimate these threats and expect not to be targeted or underestimate the scope of collateral damage. Therefore, companies need to upgrade their current business continuity and disaster recovery models to face future cyber threats.

After analyzing several cyber threat reports of the biggest cyber security firms, consultancies and government agencies and interviewing the industry experts, the results of this research are in accordance with the hypothesis.

Companies are not prepared for massive disruptive cyber threats. The government expert stated that: *"Companies are having difficulties with the organization of resilience to protect themselves to these threats."* The expert from the consultancy agreed and stated that "*almost every company doesn't get the basics right"* (regarding cyber resilient business continuity plans). The expert at the cyber security firm even added that companies do not take black swan attacks into account.

The interviewed logistics service provider had measures in place which will be enough to protect themselves from the regular cyber criminal. However, the measures would not suffice to deal with a massive disruptive cyber threat. To help companies make themselves more cyber resilient and better protected against massive cyber threats the IBCDRPCR (figure 1 in the chapter: Cyber Resilience) was proposed.

Concluding, companies do not take into account massive disruptive cyber threats in regard to business continuity and business survival. If companies want to prepare themselves against these threats, they should implement the IBCDRPCR to boost their cyber resilience since *"Boosting resilience is the most important tool in reducing risk"* (NCSC, 2019, p 6).

This research has several limitations. The first limitation is the amount of massive disruptive events that have occurred. There only have been a few of these events which make it difficult to exactly define what a massive disruptive event consists of. The threat matrix will also carry certain limitations, the reports used to create this matrix will present the most common threats, so rare threats will be left out. The break-out time which will be presented in the matrix will be an average, there will always be cyber attacks which can will have a faster break-out time.

Another limitation is the number of companies where the interviews will be conducted. Since only three companies will be interviewed, there is a chance a company which is better prepared to prevent such an event will be left out of the research. The companies themselves are also a limitation, since there is limited time for this research and there is a limited amount of companies willing to consent to an interview, my sample of companies will be small. The companies which are to be interviewed are a consultancy, a cyber security firm and a company which is a logistics service provider in the supply chain of retail businesses. Since two of the to be interviewed companies provide cybersecurity services to their customers, they can also give insight to the preparedness of their clients broadening the scope of the findings presented by the interviews.

Finally, the last limitation is that cyber threats are evolving and that measures to prevent such an event which will be found in this research can become irrelevant in a matter of months through technological advancements.

While carrying out this research, some companies indicated that they made conscious decisions to operate with a low level of cyber resilience. These companies believe that the chance they are attacked is too little to implement all kinds of expensive measures. Other companies also chose to not implement these measures but to take out a cyber security insurance. As the NCSC (2019) stated, while cyber security measures are an important defense against cyber threats, these measures cost time and money. McKinsey (2019) published the article *"The risk-based approach to cybersecurity"* this October. They prefer this risk-based approach above the maturity-based approach which is the de facto standard. The risk-based approach means that the companies should reduce the specific elements of cyber risk, therefore they will *"no longer "build the control everywhere"; rather, the focus will be on building the appropriate controls for the worst vulnerabilities, to defeat the most significant threats—those that target the business's most critical areas"* (Boehm et al, 2019). Therefore, further research should be conducted in the light of the new risk-based approach to cyber security.

Concluding, companies see massive disruptive cyber threats as threats which disrupt the business continuity and bring the survival of the targeted or infected company in danger with a realistic chance of happening. These are: 1) Cyber espionage by state actors. 2) Cybercrime-as-a-service offered by cybercriminals. 3) Big Game Hunting by cyber criminals and state actors. 4) Destructive attacks by state actors. Companies are not prepared for these threats and do not take them into account in regard to business continuity and business survival. To prepare against these threats, companies should implement the IBCDRPCR to boost their cyber resilience.

References

Accenture Security (2019). Cyber Threatscape Report. Retrieved from https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf.

Accenture Security (2019). The Cost of Cybercrime. Retrieved from https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf.

Accenture Security The Cost Of Cybercrime. Retrieved from https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf.

Allodi, L., & Massacci, F. (2014). Comparing Vulnerability Severity and Exploits Using Case-Control Studies. *ACM Transactions on Information and System Security (TISSEC),17*(1), 1-20.

Allodi, L., & Massacci, F. (2017). Security Events and Vulnerability Data for Cybersecurity Risk Estimation. *Risk Analysis, 37*(8), 1606-1627.

Allodi, L., Etalle, S., Security Embedded Networked Systems W&I, & Security. (2017). Towards realistic threat modeling : Attack commodification, irrelevant vulnerabilities, and unrealistic assumptions. *SafeConfig '17 Proceedings of the 2017 Workshop on Automated Decision Making for Active Cyber Defense, 3 November 2017, Dallas, Texas,*23-26.

Allodi, L., Massacci, F., Williams, J., Security Embedded Networked Systems W&I, & Security. (n.d.). The work-averse cyber attacker model : Theory and evidence from two million attack signatures. 16th Annual Workshop on the Economics of Information Security (WEIS 2017), (16), *16th Annual Workshop on the Economics of Information Security* (WEIS 2017), 2017, Issue 16.

Aven, T. (2013). On the meaning of a black swan in a risk context. *Safety Science, 57,* Safety Science, Aug 2013, Vol.57.

Boehm, Jim, Curcio, Merrath, Shenton, and Stähle (2019). The risk-based approach to cybersecurity. McKinsey. Retreived from https://www.mckinsey.com/business-functions/risk/our-insights/the-risk-based-approach-to-cybersecurity.

Cerullo, Virginia, & Cerullo, Michael J. (2004). Business Continuity Planning: A Comprehensive Approach. *Information Systems Management, 21*(3), 70-78.

Check Point Research (2019). Cyber Attack Trends Analysis Key Insight to Gear up for in 2019: 2019 Security Report Volume 01. Retrieved from http://snt.hr/boxcontent/CheckPointSecurityReport2019_vol01.pdf.

Cherdantseva, Burnap, Blyth, Eden, Jones, Soulsby, & Stoddart. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security, 56*(C), 1-27.

Conklin, W., & Shoemaker, D. (2017). Cyber-Resilience: Seven Steps for Institutional Survival. *EDPACS, 55*(2), 14-22.

CrowdStrike (2019). Global Threat Report: Adversary Tradecraft and the Importance of Speed. Retrieved from https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/.

CrowdStrike Services (2018). CrowdStrike Services Cyber Intrusion Casebook 2019: Stories from the Front Lines of Incident Response in 2018 and Insights that Matter for 2019. Retrieved from https://www.crowdstrike.com/blog/the-crowdstrike-services-cyber-intrusion-casebook-2018-offers-compelling-stories-from-the-front-lines-of-incident-response/.

De Crespigny, M. (2012). Building cyber-resilience to tackle threats. *Network Security,2012*(4), 5-8.

Geenberg, A. (2018, August 22). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Retrieved from https://www.wired.com/story/notpetya-cyberattackukraine-russia-code-crashed-the-world/.

Geenberg, A. (2018, August 22). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Retrieved from https://www.wired.com/story/notpetya-cyberattackukraine-russia-codecrashed-the-world/.

Gibb, F., & Buchanan, S. (2006). A framework for business continuity management. *International Journal of Information Management*, 26(2), 128-141.

Jasper, S. (2017). U.S. Cyber Threat Intelligence Sharing Frameworks. *International Journal of Intelligence and CounterIntelligence, 30*(1), 53-65.

Kaspersky Lab Daily (2018, November 6) Top 5 Most Notorious Cyberattacks. Retrieves from https://www.kaspersky.com/blog/five-most-notorious-cyberattacks/24506/.

Kunreuther, H. (2002). Risk Analysis and Risk Management in an Uncertain World 1. *Risk Analysis, 22*(4), 655-664.

Lipson, H., & Fisher, D. (1999). Survivability-a new technical and business perspective on security. *Proceedings of the 1999 Workshop on New Security Paradigms,* 33-39.

Llave, M. (2018). Data lakes in business intelligence: Reporting from the trenches. *Procedia Computer Science*, *138*, 516-524.

Mattern, T., Felker, J., Borum, R., & Bamford, G. (2014). Operational Levels of Cyber Intelligence. *International Journal of Intelligence and CounterIntelligence, 27*(4), 702-719.

Maurer, T. (2018). *Cyber mercenaries : The state, hackers, and power*.

McAfee (2019). McAfee Labs Treats Report, August 2019. Retrieved from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf.

Muniz, J. (2016, February 16). Responding to Real-World Cyber Threats. *CISCO*. Retrieved from http://www.ciscopress.com/articles/article.asp?p=2481826.

National Coordinator for Security and Counterterrorism (2019). Cyber Security Assessment Netherlands CSAN 2019. Retrieved from https://english.nctv.nl/documents/publications/2019/06/12/cyber-security-assessment-netherlands-2019.

Pat.-Cornell, E. (2012). On "Black Swans" and "Perfect Storms": Risk Analysis and Management When Statistics Are Not Enough. *Risk Analysis*, 32(11), 1823-1833.

Rao, N., Poole, S., Ma, C., He, F., Zhuang, J., & Yau, D. (2016). Defense of Cyber Infrastructures Against Cyber-Physical Attacks Using Game-Theoretic Models. *Risk Analysis, 36*(4), 694-710.

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, 35(1), 5-32.

Sahebjamnia, Torabi, & Mansouri. (2015). Integrated business continuity and disaster recovery planning: Towards organizational resilience. *European Journal of Operational Research, 242*(1), 261-273.

Stanton, Stam, Mastrangelo, & Jolton. (2005). Analysis of end user security behaviors. *Computers & Security*, 24(2), 124-133.

Symantec (2019). Internet Security Threat Report Volume 24 | February 2019. Retrieved from https://www.symantec.com/security-center/threat-report.

Taleb NN. (2007) The Black Swan: The Impact of the Highly Improbable. New York: *Random House*.

Taylor, H. (2018). What are cyber threats: how they affect you and what to do about them. Retrieved fromhttps://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/.

WRR. (2019). Voorbereiden op digitale ontwrichting. *Wetenschappelijke Raad Voor het Regeringsbeleid.* Retrieved from https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting.

Appendix

Interview questions

Subjects regarding massive disruptive cyber threats

- *What are the biggest cyberthreats?*
- *Largest cyber risks from the past five years?*
- *What trends do you see in the cyber threat landscape and how do you see it evolving over the next five years?*
- *What are your classifications for a massive disruptive threat?*

Previously occurred massive disruptive cyber threats

- *What cyber attacks do you know?*
- *What cyber attacks has your company experienced?*
- *If so, how were they handled?*
- *How would you handle the threats from the threat matrix, are you well enough prepared?*
- *How would you have dealt with previous massive cyber threats? (NotPetya, WannaCry)*

Cyber resilience of the company

- *How do you prepare for these threats?*
- *How is your cyber security is arranged?*
- *What are your response strategies?*
- *Do they have business continuity / disaster recovery models in place?*
- *What is the response time for such an event?*

Codebook on Massive Disruptive Cyber Threats

Names:	Michiel van der Steeg
Research Question:	What are massive disruptive cyber threats?
Unit of Analysis:	Paragraphs

Codebook

Code	Category	Definition	Indicators
1	Cyber Threats	Malicious acts which seek to damage data, steal data or the digital infrastructure of a company.	It includes statements about malicious acts which seek to damage or steal data. It includes statements about malicious acts which seek to disrupt the digital infrastructure of a company.
2	Threat Actors	The actors targeting specific companies for a cyber attack.	It includes statements about malicious actors who target companies with a cyber threat.
3	Scope of the threat	The level of the threat, does the threat harm business continuity and does it bring the survival of the targeted company in danger.	It includes statements about the damage the threat poses
4	Break-out time	The time the threat actors need to infiltrate the infrastructure of the targeted company and set up their attack.	It includes statements about the time it takes for threat actors to infiltrate the digital infrastructure of a company It includes statements about the time it takes for cyber attacks to harm the business continuity of survival of the targeted company in danger

Coding Rules:

- Paragraphs are only marked when it indeed poses a security threat which implies massive disruption.
- Categories are coded as much as they apply