Towards a Cyber-Resilient Crisis Management Program

An analysis of how the pre and post factors of cyber crisis response influence organizational resilience

By Erik Evert Veldhuis, s1749196

Supervisor: T. van Steen

Second Reader: S. Schinagl

Abstract

Crisis management research recognizes the opportunities that lie in examining cyber crisis management, yet approaches in a standardized way. Over the past decades, information security has given rise to cyber security, resulting in the need of significant understanding of cyber security threats. The increasingly complex cyber risk landscape requires organizations to take appropriate steps in increasing organizational cyber security resilience through cyber crisis management. To understand what is essential to cyber crisis management, risk and crisis management must be understood. Consequently, to indicate how these concepts are translated into the cyber domain the British Standardization Institution (BSI) framework and the Situational Crisis Communications Theory (SCCT) are analyzed and broken down into pre and post factors. Pre factors characterized by the repression of risks through preparation and post factors illustrated by the mitigation of negative externalities through response and recovery. Research is conducted through a multiple case study of two organizations, complemented by interview and documentary data. The main findings partially indicate that mature cyber security organizational structures, cooperative information sharing and reflective learning positively influence an organizations' cyber crisis response. Full support is found for the integration and alignment of cyber security programs within all layers of the organization, the need for training of crisis leadership and the necessity of transparent crisis communication strategy.

Key words: Cyber, cyber resilience, cyber security, cyber risk management, cyber crisis management.

Acknowledgements

I would like to express my sincere gratitude to the Cyber Security executive degree at Leiden University and the individuals responsible for making the program such a success. I am thankful to my supervisors, Tommy van Steen and Stef Schinagl for their continuous time, guidance and support. With their support the research process was constructive and insightful.

I am extremely grateful to my employer who provided me with the opportunity to further deepen my knowledge in the domain of cyber security, as well as to my colleagues from all over the world, with whom I can share information regarding the ever-evolving and important topic of cyber crisis management.

Lastly, I am fully indebted to my friends, family and especially my significant other for helping me cope with all that comes with studying and pushing me further than I thought I could go.

Table of Contents

1. Introduction

The digital transformation from information security to cyber security is one of the most prominent contemporary topics, as the digital economy rises along with unprecedented threats in the cyber realm (Huang, Siegel, & Madnick, 2018; Lee, 2018; Nobles, 2018; Čelik, 2019). Scholars call for the need of security measures and responses, as the cyber domain creates "new vulnerabilities with far reaching implications" (Spremić & Šimunic, 2018, p. 341). The cyber domain's increasing presence as a database and networking space has generated new forms of business (Zhang, et al., 2015). Yet, despite driving innovation the integrated nature of cyber space increases disrupting impacts on organizations (Shaheer & Li, 2020) (Spremić & Šimunic, 2018) (Spremić, 2017). Consequently, central to the development of the digital economy is cyber security, as "it takes 20 years to build a reputation and few minutes of cyber-incident to ruin it" (Nappo, 2019).

Over the past decades, the changing threats within the cyber landscape have put enormous pressure on organizations in both the public and private domain. The list of organizations that have been a victim of cyber-related threats is long, as it is estimated that approximately 32 percent of companies have been affected by cybercrime (Huang, Siegel, & Madnick, 2018). It is projected that the costs of cybercrime will grow from an annual $3 trillion in 2015, to $6 trillion by the year 2021 (Huang, Siegel, & Madnick, 2018). The numbers above reflect Mueller (2012), the former FBI Director's statement that there are only two types of companies, those that have been hacked and those that will be.

Consequently, new challenges are faced in how cyber crisis are best responded to, inducing developments within the cyber security domain. Scholars opt for support in responding through the use of the standards from the BSI framework and the SCCT. The BSI framework establishing a basis for crisis management frameworks and the SCCT being reflected in response strategies, which have proven to be of great importance in establishing resilience from crisis outside the cyber realm. It is within these frameworks that the pre and post factors of response can be identified. Pre response factors pertaining to the preparation of potential cyber crisis management and post factors reflecting the response and recovery phases. More specifically, through incorporating both pre and post factors scholars and organizations attempt to move towards a form of cyber resilience. Cyber resilience being the "ability to withstand, contain, and rapidly recover from a cyber incident by anticipating and adapting to cyber threats" (Zhang, Collins, & Connor-Close, 2020, p. 3). Accordingly, cyber crisis resilience is reflected within cyber crisis management, as it encompasses the "ability to adequately prepare, respond and to recover cyber crisis" (Zhang, Collins, & Connor-Close, 2020, p. 2).

It is the pressure from the evolving digital economy that calls for this resilience, one that can be established through the development of cyber orientated crisis management. Yet actions, as well as research remains fragmented. The resemblances in the nature of crisis, as "an event perceived by managers and stakeholders as highly salient, unexpected, and potentially disruptive [that] can threaten an organization's goals and have profound implications" (Bundy, Pfarrer, Short, & Coombs, 2017, p. 1662), has resulted in overlooking important case specific aspects central to responding to crisis in the cyber realm (Wang, Wang, & Gwebu, 2018). It is the ever evolving, highly contagious and unpredictable nature that sets cyber risk apart from other more conventional operational risk (Jai & Chen, 2019). Consequently, research within cyber security has "only begun to scratch the surface" (Vieane, et al., 2016, p. 770). Despite the BSI framework being labeled as best practices, it remains just the "starting point of thinking for many information security experts" (Berg, 2017, p. 1), partially neglecting essential cyber pre and post response elements. Theories such as the SCCT fail to explore "human factors in cybersecurity [that] threatens the existence of every business" (Calvin, 2019, p. 1), ignoring the importance of leadership qualities and communication styles. Further, the significance of the structural integration of cyber is not investigated, even though the current chronic shortage of cyber security professionals has already proven to further amplify the cost of cyber resilience (Zhang, Collins, & Connor-Close, 2020). Therefore, even though effective cyber crisis management is crucial to maintaining an organizations operation, uncertainties remain in understanding and establishing cyber crisis response (Zhang, Collins, & Connor-Close, 2020).

Research as to how cyber crisis resilience can be established remains disintegrated, as it often focuses on general forms of threats along with cyber investment optimization. In turn neglecting "variability and risks that the humans would include in a real situation" (Carías, Labaka, María, Sarriegi, & Hernantes, 2019, p. 2; Chang, Dybes, & Moore, 2015). Research is fragmented as crisis management models such as the BSI framework and the SCCT overlook the complexities and intangible nature of crisis in the cyber realm, indicating the need for continuous cyber crisis examination. Therefore, this research argues that the current literature on the role of cyber crisis management’s pre and post factors remains fragmented. Consequently, the following research gaps are addressed.

Firstly, the gap regarding the necessary advancement of research within the cyber domain must be addressed. While many studies have been conducted in the field of crisis management, the aspect of cyber is not widely examined within crisis management, as it is often deemed too complex (Spremić & Šimunic, 2018). Starting with establishing the definition, it being “one of the most fundamental challenges [due to] the lack of a precise and universal definition that clarifies which activities should be included when measuring the digital economy” (Barefoot, Curtis, Jolliff, Nicholson, & Omohundro, 2018, p. 6). Consequently, scholars state that the “foundational knowledge upon which the field of cyber security is being developed is fragmented” (Rashid, et al., 2018, p. 96). Leading to the field primarily focusing on general crisis origins such as disruptive and poorly managed incidents, as well as latent problems (British Standard Institution, 2014).

Secondly, the link between cyber risk management and cyber crisis management remains lacking. Research on cyber risk management is advanced, yet when transitioning from risk towards crisis it becomes unclear who is responsible (McKinsey & Company, 2019). The BSI framework and the SCCT set the stage for understanding cyber risk. However, once risks escalate the complex environment in which organizations operate, a solution is required in responding to the continuing changing cyber risk landscape. The gap being created by the complexity of the landscape, as well as the sole focus “on technological aspects of cyber, acknowledging the human in passing, if at all” (Vieane, et al., 2016, p. 770). While there has been an increasing focus on cyber security in the academic world, as well as in public and private organizations, the link with business continuity and effective crisis management remains thin as prioritization is lacking (McKinsey & Company, 2019).

Lastly, the incomplete approach from cyber risk to crisis management has resulted in partial cyber crisis management frameworks. Research remains superficial as there “still exists a major gap in the field between understanding of the domain and currently available research meant to address relevant issues” (Vieane, et al., 2016, p. 770). While crisis management research elaborates on what factors contribute to an effective crisis response, due to the nature of cyber crisis, these cannot be compared equally. Consequently, there are limitations to understanding what pre and post response phase factors influence effective cyber crisis management.

Therefore, by critically assessing the current gaps in cyber crisis management frameworks the influence of unique situational factors can be captured.

In understanding the relevance of these gaps, new research opportunities emerge. By bringing together the analysis of cyber crisis and the current risk and crisis management thereof, the influence of pre and post factors can be better understood. Opportunities lie within the topic of this research in understanding how effective and integrated cyber crisis management can be developed. Therefore, the following research question is addressed:

RQ: How do the pre and post factors of cyber crisis management influence organizations cyber resilience?

In order to analyze the pre and post factors that influence the development of cyber crisis management the thesis is structured as follows. Firstly, the theoretical background central to this study is introduced. The transition from information security to cyber security is examined, as well as the basis of risk management. By comparing risk management and crisis management to that within the cyber domain the research gaps can be addressed. Following, the BSI framework and SCCT are addressed, to identify what factors are central to cyber crisis management. Secondly, the methodology section presents the study's qualitative multiple case study research design, defining the sample of two cyber crises and the data analysis strategy. The study purposely selects two cases allowing a within and cross-case analysis. Thirdly, the results section presents the analysis of the influence of the pre and post factors of cyber crisis management on organization resilience. Accordingly, these results are discussed in-depth and lead to the final concluding section of this study.

2. Literature Review

The topic of cyber crisis management is becoming increasingly relevant with the rapid transition of society to the digital spheres of influence (Wirfs & Eling, 2019). To understand cyber risks and crisis, as well as the response and management of such, the first section examines the transition from information to cyber security. Second, risk management is introduced, highlighting the distinctive differences between risk and cyber risk management. In turn, the third and fourth section critically assess the presence of crisis management in the cyber realm. Lastly, by further identifying the unique conditions that cyber crisis are prone to, the conditions for successful cyber crisis management can be categorized into pre and post factors. This allows the conditions that are vital to cyber crisis management to be examined.

2.1. From Information Security to Cyber Security

The online transition of people, systems and structures has caused a shift in the domain of information security. Information security having once been the starting point in aiming to secure the confidentiality, integrity and availability of information, now needing to be expanded to encompass risks from the cyber realm (SANS, 2020; Berg, 2017). The basis of the field of information security and its use in “preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information” (Chandini, 2020, p. 33), has allowed new areas of investigation to arise. The increasing dependence on technologies and the interconnectedness of systems have introduced the domain of cyber security. This field of study gaining its importance as incidents within the domain, whether by accident or intentional, have the potential to disrupt society (Boeke, 2017).

Over the past decades, the term cyber security has been introduced to specify topics within information security. The increasing interconnectedness of society and organizations has given rise to the digital economy. Organizations’ agendas becoming defined by the “integration and simultaneous application of… ready-to-use digital technologies” (Spremić & Šimunic, Cyber Security Challenges in Digital Economy, 2018, p. 1). Consequently, increasing activity within cyber space, as organizations expect “digital technologies to make an increasing strategic contribution to their overall business in the coming decade” (Spremić & Šimunic, 2018, p. 341) (Bonnet, Ferraris, Westerman, & McAfee, 2012). Nevertheless, these changes in organizations operational structures do not come without risks. As “security challenges are different from those in traditional network environments, and need to be further studied” (Zhang, et al., 2015,

p. 17). Effects of cyber-attacks are being felt in all sectors and aspects of society. Damages including reputational and financial loss (Shukla & Nagurney, 2016). Therefore, this changing landscape calls for new security and crisis management measures.

Yet, the definition of cyber security requires clarity, as it goes beyond the boundaries of information security and can no longer be used interchangeably with the term information security. The cyber space consists of multiple layers, as it includes the protection of information resources, as well as other assets including the person themselves (Klimburg & Mirtl, 2012). In cyber security the human factor must be examined in great detail, as they are often the potential targets of cyber-attacks or even unknowingly participating in a cyber-attack (Niekerk & Solms, 2013). Consequently, cyber security can be considered "the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace- enabled systems from occurrences that misalign de jure from de facto property rights" (Purse, Thibault, & Craigen, 2014, p. 13). Focusing on these specific aspects will allow the further integration of cyber security into the domain of information security, as well as an improved analytical approach towards cyber risk and cyber crisis management to be developed. Cyber risk management has increasingly gained importance as incidents in cyberspace go further than those in the physical world. This is due to the fact that cyber incidents are not limited by time and physical boundaries. When organizations are targeted for cyber-attacks by hacktivists, terroristic groups, corporate actors, or state actors, the impacts may be financial, regulatory or reputational in nature (KPN et. al., 2020). If incidents cannot be handled in the regular incident management process, they need to be addressed by an effective crisis management response (KPN et. al., 2020). Therefore, cyber crisis management prepares organizations for the situations that cannot be dealt with in an ordinary manner and threaten the continuity of an organization. Thus, highlighting that the basis of cyber security is integral to understanding cyber risk and cyber crisis management.

2.2. Cyber Risk Management

To understand the conditions that influence cyber crisis response the concept of cyber risk management must be addressed. Cyber risk management can be understood as "the practice of identifying and analyzing potential risks in advance and taking precautionary steps to limit risk" (Giat & Dreyfuss, 2020, p. 77). This has arisen from the changing threat landscape and increasing adoption of technology, that made cyber security a politized topic within all levels of organizations (Kolini, 2017). Cyber risks are becoming increasingly relevant within our society, yet remain difficult to assess due to the absence of reliable data and research (Wirfs & Eling, 2019). Within these initial assessments an often-integrated view of cyber risk management is that of van den Berg (2017), as it successfully introduces a three-layered approach to cyber security. The layers within this approach constituting different activities in cyber space, which are subject to their own risks. Specifically, van den Berg (2017) makes a division in cyberspace between: (1) the technical layer, (2) the socio-technical layer and (3) the governance layer. As illustrated in Table 1 the increasing adoption of technology has resulted in the use of it in all domains.

Layer	**Activity**	**Potential Risks**
Technical Layer	Information Technology (IT) services and the protection of information's confidentiality, integrity and availability.	Risks to ICT systems that arise from the technical layer. For example, potential vulnerabilities in information systems or other technical related risks.
Socio- Technical Layer	The interaction between people and systems.	Risks that result from the interaction between people and systems, both intentional as unintentional. Examples consisting of the (un)intentionally deleting of data or clicking on phishing links.
Governance	The formulation of risk levels and measures to reduce cyber risk to acceptable levels.	If risks levels are not assessed correctly, appropriate measures to reduce the cyber risks are not in place.

Table 1: Exemplary Risks and Layers

Source: Adapted from van den Berg (2017)

Moreover, van den Berg (2017) successfully integrates the risk management cycle adopted by the International Organization for Standardization (ISO), into a cyber risk management cycle. By introducing a key risk management framework to the cyber domain, a solid basis is set for best practices. Table 2 further illustrates van den Berg's (2017) translation of the ISO 31000 risk management cycle to the cyber security domain.

	Risk Management	**Cyber Risk Management**
1	Establishing the context	Identify the critical cyber activities
2	Risk identification	Identify and assess their cyber risk
3	Risk analysis	Define acceptable cyber risk levels
4	Risk evaluation	Decide ways of dealing with the risks
5	Risk treatment	Design and implement cyber risk measures
6	Monitoring and review	Monitor effectiveness

Table 2: Risk Management Translated into the Cyber Domain

Source: Adapted from International Standard Organization (2018) & van den Berg (2017)

Further the importance of cyber risk management resides in its close connection to business continuity. As when combined, business continuity management and risk management have the potential to reduce risk and the potential negative effects of a disruption (International Standard Organisation, 2012). Risk management is seen as an integral part of the Business Continuity Management Cycle (BCMS), as it is considered to systematically identify, analyze and evaluate the risk of disruptive incidents to the organization. Within the BCMS cycle, the Business Impact Analysis (BIA) is conducted to assess the impacts of disrupting activities that support the organization's products and services (International Standard Organisation, 2012). Consequently, the management cycles or processes that deal with cyber risk management and BCMS are closely aligned. Yet, gaps remain as the topic of business continuity aims to "protect against, reduce the likelihood of occurrence, prepare for, response to, and recover from disruptive incidents when they arise" (International Standard Organisation, 2012, p. 1). Whereas risk management focuses on "the practice of identifying and analyzing potential risks in advance and taking precautionary steps to limit risk" (Giat & Dreyfuss, 2020, p. 76). Thus, both risk and business impact assessments are needed to attain complete business continuity strategy and implementation without conducting both a risk assessment and a business impact analysis (Long, 2017). Yet, as cyber risk management is being successfully developed, the connections towards and within cyber crisis management remains fragmented. Thus, cyber crisis management being interconnected to cyber risk management, must be further examined, as addressed in the following section.

Characteristics	Incidents	Crisis
Predictability	Incidents are generally foreseeable and amenable to pre-planned response measures, although their specific timing, nature and spread of implications is variable and thus unpredictable in detail.	Crises are unique, rare, unforeseen or poorly managed events, or combinations of such events, that can create exceptional challenges for an organization and are not well served by prescriptive, pre-planned responses.
Onset	Incidents can be without or with short notice disruptive events. Or they can emerge through gradual failure or loss of control. Recognizing the warning signs of potential, actual or impending problems is critical to incident management.	Crises can be sudden onset, without notice or emerge from an incident. Incidents that have not been contained, have escalated with immediate strategic implications or arise when latent problems within an organization are exposed, with profound reputational consequences.
Urgency and Pressure	Incident response usually spans a short time frame of activity and is resolved before exposure to longer-term or permanent significant impacts on the organization.	Crises have a higher sense of urgency and might require the response to run over longer periods of time to ensure that impacts are minimized.
Impacts	Incidents are adverse events that are reasonably well understood and thus are amenable to a predefined response. Their impacts are potentially widespread.	Due to their strategic nature, crises can disrupt or affect the entire organization, thus transcend organizational, geographical and sectoral boundaries. Crises tend to be complex and inherently uncertain, due to for instance a decision being made with incomplete, ambiguous information, the spread of impacts is difficult to assess and appreciate.
Media Scrutiny	Effective incident management attracts little, but positive, media attention where adverse events are intercepted, impacts rapidly mitigated and regular business is quickly restored. Yet, this is not always the case and negative media attention, even when the incident response is effective and within agreed parameters, has the potential to escalate an incident into a crisis.	Crises are events that cause significant public and media interest, with the potential to negatively affect an organization's reputation. Coverage in the media and on social networks might be inaccurate in damaging ways, with the potential to rapidly and unnecessarily escalate a crisis.
Manageability through Plans and Procedures	Incidents can be resolved by applying appropriate, predefined procedures and plans to intercept adverse events, mitigate their impacts and recover to normal operations. Incident responses are likely to have available adequate resources as planned.	Crises, through a combination of their novelty, inherent uncertainty and potential scale and duration of impact, are rarely resolvable through the application of predefined procedures and plans. They demand a flexible, creative, strategic and sustained response that is rooted in the values of the organization and sound crisis management structures and planning.

Table 3: Difference between Incidents and Crisis, BS 11200, 2014

Source: British Standard Institution (2014)

2.3. Assessing Crisis Management

Having examined cyber risk management, allows the consideration of the transition from risks to crisis. Yet, cyber crisis management remains fragmented within the domain of crisis management. Therefore, to fully understand the differentiators within cyber crisis management, first crisis management theories and approaches must be understood. By assessing the challenges that are encountered in crisis management and to what extent these are applicable to cyber situations, the basis of cyber crisis management can be effectively analyzed.

To further clarify the difference between risk and crisis management the term crisis must be defined, as well as the difference between what constitutes an incident or crisis. A crisis can be defined as “an event perceived by managers and stakeholders as highly salient, unexpected, and potentially disruptive [that] can threaten an organization’s goals and have profound implications for its relationships with stakeholders” (Bundy, Pfarrer, Short, & Coombs, 2017, p. 1662). The difference between an incident or crisis is illustrated above in Table 3, as it is of utmost importance when effectively dealing with a crisis, that there are clear guidelines on the distinction between what is an incident and what qualifies as a crisis.

Further, two primary perspectives of crisis management are identified. Namely, the internal perspective focusing on managerial systems within an organization, and the external perspective, concentrating on the interactions between organizations and their stakeholders (Bundy, Pfarrer, Short, & Coombs, 2017). The importance of these perspectives being reflected in the fact that often immediate action is required, as crisis are situations that cannot be dealt with within the regular organization’s processes and require the input or management by a crisis team.

With regards to crisis management there are multiple theories and international standards, the ISO 22361 standard on security and resilience and the British Standard (BS) 11200 standard on crisis often being seen as leading. The BS 11200 highlights that the factors “necessary to create a crisis management capability, [are] organized around anticipation and assessment, preparation, response, recovery, and review and learning” (British Standard Institution, 2014, p. 8). More specifically, these elements reflecting the pre and post factors within crisis, thus are central to the foundational basis of this study. Pre factors being characterized by their preparatory process-oriented nature, as anticipation, assessment and preparation are leading.

Whereas, post factors are interpreted as the core tasks of leadership, as sense, meaning and decision making are key. Figure 1 sets out the general framework for crisis management, incorporating the influence of pre and post factors.

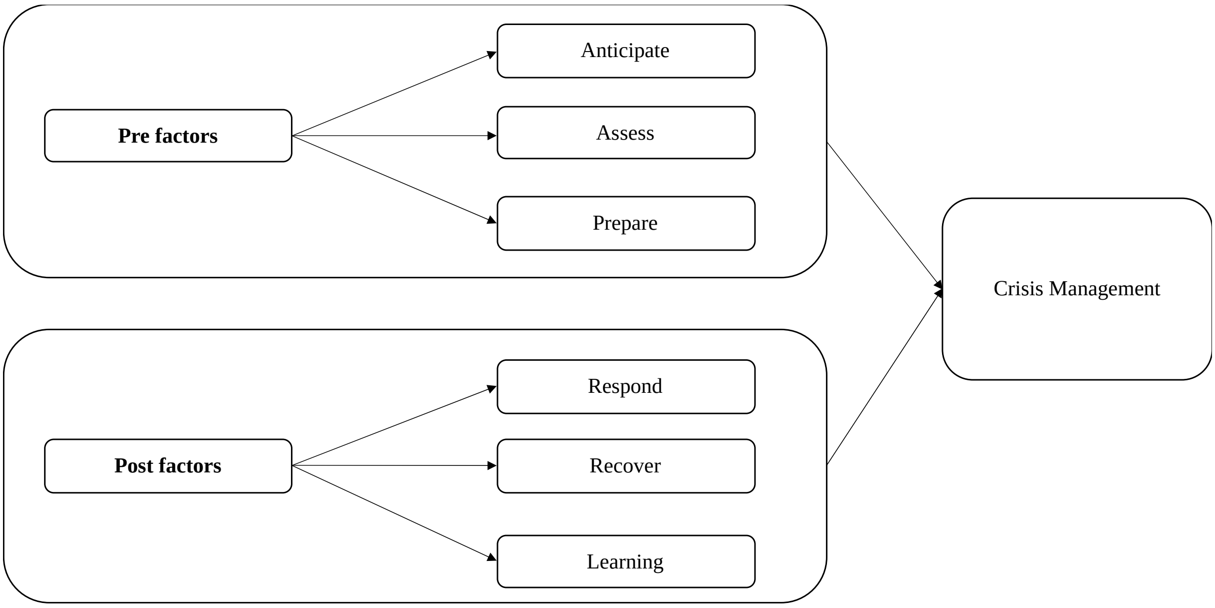

Figure 1: Framework for Crisis Management

Source: Adapted from British Standard Institution (2014)

Having outlined the framework for crisis management, the influence of SCCT within post factors must be considered, as “understanding how stakeholders will respond to the crisis informs the post-crisis communication” (Coombs, 2008, p. 163). The SCCT seeks to use research and theory to develop recommendations for the use of crisis response strategies. Crisis response strategies are matched to the nature of the crisis situation, by matching the level of responsibility and aid to victims (Coombs, 2008). The amount of reputational damage a crisis situation can inflict thus driving the selection of the crisis response strategy. The SCCT holds that the potential reputational damage from a crisis is a function of crisis responsibility and of intensifying factors. A review of these factors sets the stage for a discussion of how to assess the reputational threat posed by a crisis situation (Coombs, 2008). By understanding the influence of SCCT within post factors, specifically the response phase, the unique conditions of crisis can be better assessed.

The conditions within Figure 1 reflect the pre and post response phases of crisis management, and thus that of cyber crisis management and so provide the foundational basis for this study.

The first two conditions within the pre phase, anticipate and assess can be interpreted as the outcome of preparation. As preparation refers to the outcome of initial steps taken, therefore the research focuses on the factors within preparation. Consequently, the preparation phase factor reflects the pre factor of cyber crisis management response. Additionally, learning within the post phase can be interpreted as part of the recovery phase, therefore is integrated in the post factor of recovery. Consequently, the post factors of crisis management response that are examined are respond and recover. After the nature of cyber crisis management is further examined, this framework is further broken down and used to understand the influence of pre and post factors.

2.4. Cyber Crisis Management

Having understood the essential factors that are defining within crisis management these must be translated into the cyber domain. It being essential to take a separate look at cyber events, as these can sometimes not be dealt with in the regular incident management process. Therefore, cyber incidents are expanded upon to further allow the assessment of cyber crisis management.

The intangible and changing nature of cyber threats require a different approach in preparing and acting upon cyber incidents that have the potential to turn into a crisis. The following factors are unique for cyber related crisis and in turn affect crisis management. Namely, the digital and intangible nature of cyber incidents, making early recognition and sensemaking more difficult. The security challenges being different than “those in traditional network environments” (Zhang, et al., 2015, p. 18), as incidents in cyberspace are not limited by physical boundaries and time due to interconnected nature over systems. Additionally, cyber aspects differ due to its rapidly developing domain, unfortunately in which criminals take advantage of the potential gaps in the “realm of dynamic information transmittal” (Vieane, et al., 2016, p. 770). Consequently, cyber incidents have the potential to escalate in a way that is unseen with other incidents. For example, ransomware attacks have become a serious threat to individuals, organizations and governments. Ransomware attacks are considered to be ‘a particular class of scareware that locks the victims ‘computers until they make a payment to re-gain access to their data’ (Grill, Bacs, Platzer, & Bos, 2015, p. 3). Another example of cyber threats is the creation of fake profiles “to exploit the operational vulnerability that arises” (Huang, Siegel, & Madnick, 2018, p. 705). While cyber incidents are common, incidents that reach crisis levels can result in an unexpected amount of damage. Besides the formation of an incident response team, organizations need to establish the capability to adequately prepare for, responding to and recovering from cyber inflicted crisis (Golandsky, 2016). Due to the dynamic cyber risk landscape, cyber crisis management is a unique and challenging field of study.

With regard to crisis management the BS 11200 (2014) provides good practices, with its procedural steps covering the preparatory stages, as well as guidelines for an effective crisis response. Further, within crisis management the SCCT focuses on the factors that influence an organizations reputation in their crisis response. While the BS 11200 (2014) and SCCT can be applied to cyber crisis management they are limited in their scope. With regard to the BS 11200 (2014), it misses the essential focus on cyber specific situations that have the potential to be detrimental for an effective cyber crisis response. The BS 11200 (2014) provides a framework for response, yet not the specific variables a long which to act to enable successful crisis response. Further, by applying the SCCT model on cyber crisis management, the scope only focuses on the perception of a cyber crisis response and how it is framed in the media (Nurse & Knight, 2020). Unfortunately, cyber crisis research has primary focused on communication strategies after cyber security incidents (Nurse & Knight, 2020). Research on how media interprets an organizations crisis communication in relation to the SCCT can limit an analysis in a way that it focuses on a fixed set of categories, which may overlook other important elements (Nurse & Knight, 2020). By only focusing on the communication aspect, an analysis does not include the pre situational factors on which a crisis response can be based (Nurse & Knight, 2020). Additionally, cyber related crisis appears to face greater complexities. Therefore, in assessing cyber crisis management it is essential to research the distinctive factors in cyber crisis management.

Having understood the differences that come along with a cyber crisis, it becomes vivid that cyber crisis requires its own unique approach in both preparing for and acting upon cyber crisis. By building upon the gaps, we can identify the elements that are essential for effective cyber crisis management. Therefore, to guide the assessment of pre and post factors, the conceptual model depictured in Figure 2 provides an overview of the factors examined. This model contributes to how the research question is approached, separating the factors influencing cyber crisis, thus guiding the following research. Due to the time frame and scope of this research, and as previously mentioned the framework is broken down and steps are integrated into phases of prepare, respond and recover. By separating these principles into the pre and post factors these can be further analyzed in the following section.

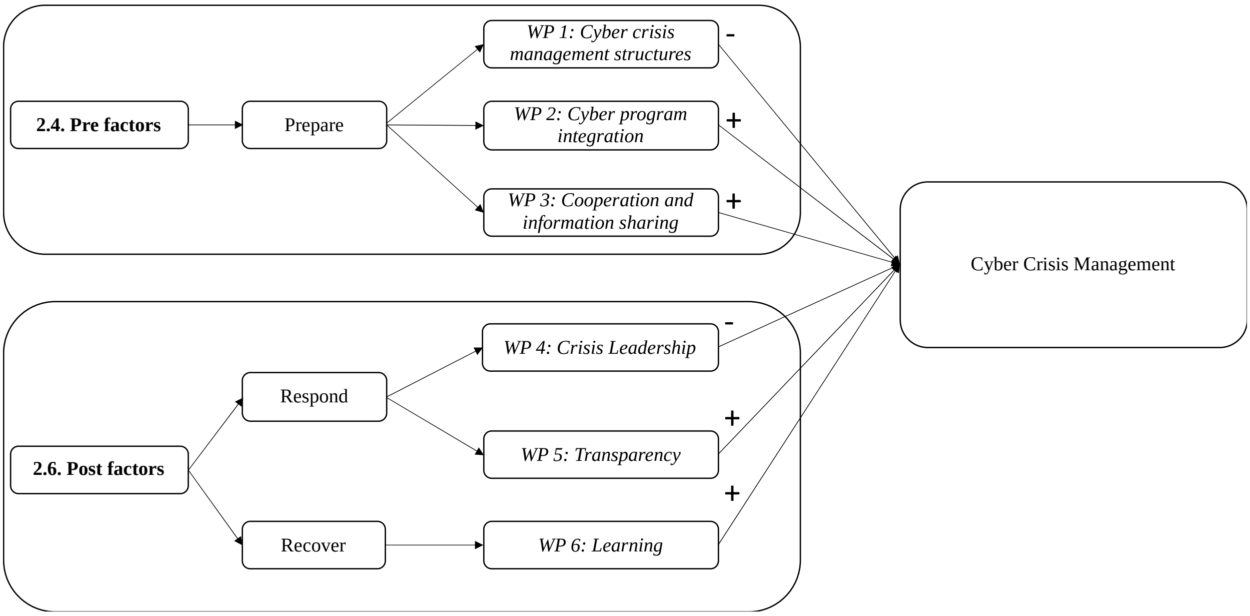

Figure 1: Conceptual Model, the Influences of Crisis Managements' Pre and Post Factors on Cyber Crisis Management

Source: Author

2.5. Pre Response Factors

Within the response phase pre factors can be identified as the variables that influence an organization's crisis preparedness. Such factors being of great importance as they influence how crisis challenges are mitigated (British Standard Institution, 2014). Thus, as highlighted in Figure 2 the BSI (2014) framework is further broken down identifying the following pre factors: cyber crisis management structures, cyber program integration and cooperation and information sharing.

2.5.1. Cyber Crisis Management Structures

The first condition for effective cyber crisis management resides in the establishment of adequate cyber crisis management structures. The existence of cyber crisis management structures prior to crisis is essential for an effective response and reflected in cyber integration, the establishment of plans, as well as trainings (KPN et. al., 2020). The implementation of such aids in preventing threats to emerge and functions as repression measure, key to minimizing negative effects (Berg, 2017). In doing so, adequate cyber crisis management structures provide foundation for effective crisis response.

According to van den Berg (2017) the securing of cyber activities being a risk management challenge itself, sets forward a cyber risk management process cycle. This cycle can be used as the starting point for establishing effective cyber crisis management structures. The cyber risk management process including the following: (1) identifying cyber activities, (2) identifying and assessing cyber risk, (3) defining acceptable cyber risk levels, (4) deciding how to deal with risks, (5) designing and implementing of cyber risk measures and (6) monitoring effectiveness (Berg, 2017).

As noted in the theoretical framework, adequate incident response and crisis management structures are vital in dealing with any crisis. With regard to cyber risk, the integration of cyber is central to structure creation (British Standard Institution, 2014). Yet due to the intangible nature, as well as the continuous isolation of cyber risk towards the IT department this remains lacking (Berg, 2017; British Standard Institution, 2014). Moreover, similar to the BSI’s (2014) best practice crisis management, is the need for documents that describe the crisis management and business continuity processes and protocols. Yet within cyber crisis management these additional steps remain to be taken. The presence of insufficient plans being reflected in improvised and decentralized cyber crisis responses (Backman, 2020). Furthermore, organizations may have incident management processes in place for IT related risks. However, an additional cyber crisis management process is needed together with its rehearsal, to create awareness and cyber crisis resilience. As often the entry way for cyber criminals is simply through an organization’s employees (Berg, 2017). In turn, further reflecting the need for employees to have the right competencies and skills to prepare for crisis. The training of employees with regard to incidents and crisis handling being key for effectively responding to a cyber crisis (Backman, 2020), as “better situational awareness allows employees to evaluate potential risks, and then prepare and execute courses of action without negative consequences to the enterprise” (Kulikova, Heil, van den Berg, & Pieters, 2012, p. 104).

According to Amorin et al. (2013), a new approach is needed for successfully training for cyber crisis response. Yet in training stakeholders to effectively respond to cyber crisis the challenge remains in the fact that new threats appear daily (Amorim, Andler, Laere, Gustavsson, & Azevedo, 2013). Initially solely training needs were identified, yet trainings in cyber security need to be based on the reporting and explaining of new threats, combined with risk assessment. More specifically, for trainings in the field of cyber crisis management, besides the identification of learning needs, there is a need to include cyber specific learning objects that explain specific threats, technical information and include simulations explaining how to proceed step-by step to solve issues (Amorim, Andler, Laere, Gustavsson, & Azevedo, 2013).

Therefore, this leads to the development of the first working proposition (WP):

WP1: Immature cyber security organizational structures negatively influence cyber crisis response.

2.5.2. Cyber Program Integration

The second condition for effective cyber crisis management is higher level cyber program integration. There is a need for internal efficiency to respond fast and effectively through effective cyber program integration, as cyber security is becoming one of the most pressing governance issues (Nolan, Lawyer, & Dodd, 2019). The need for cyber program integration being reflected in the World Economic Forum's (2019) listing of cyber risk as one of the leading global risks. According to Lewis (2018), it is estimated that cybercrime has cost the world approximately 600 billion dollars, calculated to be 0.8% of the global GDP. Having become a strategic risk for organizations it needs to be addressed at the highest level. The protection of digital assets ultimately residing with the boards of directors and corporate executives, as the risks have the potential to reflect poorly on corporate leadership (Nolan, Lawyer, & Dodd, 2019). While there is an increasing understanding of the importance of addressing cyber risk, there is still a lack of understanding or motivation of fully integrating cyber program within an organization's governance models. Far too often cyber security continues to be dealt with by the Chief Information Security Officer (CISO) or IT managers (Thycotic, 2019). Additionally, communication and reporting often remaining superficial, leaving the board without understanding of the potential business risks (UK Department for Digital, Culture, Media & Sport, 2019).

This gap in addressing cyber risks within the board of directors, indicates the need for managing cybersecurity top down like all other major business risks (Nolan, Lawyer, & Dodd, 2019). For example, JP Morgan Chace only appointed directors with risk expertise on the board's risk committee after an incident that led to the financial loss of 6 billion in trading losses (Abelson & Kopechi, 2012). Therefore, there is a need for a central responsibility of the board for minimizing the financial damage of business disruption resulting from a cyber related incident or crisis. In doing so, there should be a balance between determining the likelihood of cyber related threats and assessments of how the organizations cyber security performs in coordination with multiple threat scenarios. As a result, the further inclusion of cyber risks within the board of directors allows for a more specific discussion with regard to what resources are available in the case of a serious cyber incident or crisis (Nolan, Lawyer, & Dodd, 2019).

In understanding the need for the further integration of the cyber function at board level, it is clear that board and executive management team performance will increasingly depend on how cyber risks, incidents and crisis are being managed (Nolan, Lawyer, & Dodd, 2019). Naturally, the further integration of an organization's cyber program or function creates awareness and knowledge regarding cyber risk and eventually results into better coordination and communication in the preparation phase, as well as during a cyber crisis response. Therefore, cyber crisis management requires a crisis management team (CMT) to quickly come up with an overview of potential consequences. Due to the complexity of a cyber crisis, effective cooperation and communication between all layers of the organization is essential and requires the integration of cyber within the crisis management program. This can be reached by the integration of the activities of the CMT, CISO office, Security Operations Center (SOC) and Computer Emergency Response Team (CERT). A faltering communication line between one of these can make the difference between a well-managed crisis and damage to the organization (KPN et. al., 2020).

Therefore, this leads to the development of the second working proposition:

WP2: The integration and alignment of the activities of the CMT, CISO office, SOC and CERT will improve an organization's cyber crisis response.

2.5.3. Cooperation and Information Sharing

The third condition for effective cyber crisis management resides in cooperation with stakeholders. The changing cyber threat landscape and the continuous interconnection and aggregation of organizations requires greater coordination in mitigating risks. The cooperation with stakeholders can be separated into the following aspects: (1) cooperation parties with integrated systems, (2) information sharing platforms, and (3) communication of data breaches (KPN et. al., 2020).

Cooperation parties in which systems are integrated refers to third party risk management or supplier management. As the increasing trend of integration of information systems has naturally increased the organizational risk landscape to include suppliers or cooperating parties in scope (Boiko, Shendryk, & Boiko, 2019). Therefore, cooperation and coordination are vital to prevent any incidents that result due to the integration of cooperating parties' information systems. To protect information systems organizations should formulate an information security baseline to which all cooperating parties need to adhere. By adhering to the baseline, all organizations that are connected to the information systems, are required to have a set minimum information security maturity. The next step in effective supplier management is the integration of a review cycle in which suppliers are audited and need to prove that they fulfill the requirements that were agreed upon. However, the adoption of the integration of information security requirements as part of third-party risk management remains limited (Vitunskaite, He, Brandstetter, & Janicke, 2019).

Further, considering the constantly changing cyber risk landscape, participation in information sharing platforms is vital to understanding the latest developments and threats emerging (Berg, 2017). By participating in such platforms, prior unknown risks can be taken into account in an organization’s risk management process, which can result in the implementation of mitigating actions, as well as revision of information security policies, business continuity or crisis management plans (Backman, 2020). In addition, due to the complexity and dependencies within cyber crisis management cooperation with parties such as the National Cyber Security Centre and specialized teams, it is key to receive information regarding the latest risks and threat actors (NCSC, 2020).

Moreover, in certain cases, government agencies need to be involved due to legal reasons or implications. For example, future EU data laws “will require notification of any personal data breach to certain authorities within very tight timeframes of 24 hours” (Kulikova, Heil, van den Berg, & Pieters, 2012, p. 104). Not only is it at times a regulation, information sharing is also seen as a lifeline (Kulikova, Heil, van den Berg, & Pieters, 2012). Therefore, it is important to find the right balance in sharing information and taking time to gather all the facts. Being transparent can provide advantages to stakeholders and benefit organizations. Finding the right balance between transparency in relation to stakeholders and the risk of information leakage is essential in effectively dealing with a cyber crisis.

Therefore, this leads to the development of the third working proposition:

WP3: A focus on pro-active cooperation and information sharing with partners and stakeholders will improve an organization's cyber crisis response.

2.6. Post Response Factors

Having investigated the influences of the pre factors on cyber crisis management, the post factors can be considered. Post factors are those variables that influence an organizations crisis response after the event. Effective response can mitigate negative externalities, reflected in terms of safety, finances and reputation. Therefore, as illustrated in Figure 2 the following post factors have been identified and are investigated: cyber crisis leadership, transparent communication and reflective learning.

2.6.1. Cyber Crisis Leadership

The fourth condition for effective cyber crisis management resides in crisis leadership. While crisis leadership remains a complex phenomenon, it has meaningful consequences and has the ability to significantly establish change (Gigliotti, 2016). Form fitted leadership has the potential to minimize negative externalities during a crisis, however, if not done correctly may worsen the situation and outcomes.

According to Boin et al. (2013) leadership in crisis management can be assessed along three dimensions. First, the ability to organize, direct and implement actions that minimize the impact of threats. Second, establishing cooperation between new partners and allowing the re-adjustment of existing processes or protocols. Third, leaders must establish direction and guidance. Leadership is an important differentiator with regard to an effective cyber crisis response, as the actions of leadership are core to success (Danet & Weber, 2020). Besides the three critical dimensions mentioned above, Boin et al. (2013) establish seven extra criteria, namely: early recognition, critical decision making, vertical and horizontal coordination, coupling and decoupling, meaning making and rendering accountability (Boin, Kuipers, & Overdijk, 2013).

What makes leadership in cyber crisis complex is the intangible and complex nature of the crisis (Boin, Hart, Stern, & Sundelius, 2017; British Standard Institution, 2014). Additionally, the SCCT solely addresses post crisis communication, it does not provide guidelines on how to lead (Coombs, 2008). Common operational frameworks for cyber crisis leadership are argued to remain lacking, as elements such as the pace of threat and recovery are often uncertain (British Standard Institution, 2014). What further categorizes cyber crisis leadership as complex, is the lack of confinement of the crisis and the amount of data that is needed to process crisis related information (Backman, 2020). These issues and the everchanging landscapes of cyber crisis could be overcome through trainings that opt for awareness and guide actions (Knight & Nurse, 2020; Backman, 2020). Trainings are essential as they focus on the human aspect within crisis management (British Standard Institution, 2014). Therefore, the mobilization of technical expertise and creativity, improvisation and pragmatic thinking, are important preconditions for the efficient managing of cyber crisis (Backman, 2020). Leadership in crisis within the cyber domain requires more than trust and atomy, as adequate knowledge through training in this complex domain is key.

Therefore, this leads to the development of the fourth working proposition:

WP4: Untrained crisis leaders have a negative influence on a cyber crisis response.

2.6.2. Transparent Communication

The fifth condition for effective cyber crisis management is transparency in communication. Just as in any other crisis, communication between organizations, citizens and stakeholders is key (Boin, Kuipers, & Overdijk, 2013). The quick transfer of correct information to the public and gaining control of the narrative is vital in managing a cyber crisis effectively (Backman, 2020). Incorrect communication "can cause more damages than the crisis itself" (Bakos, Dumitras, & Harangus, 2019, p. 2). Therefore, information needs to come from the organization and be "an integral part of the organization's response to any crisis and cover all means of communication, both internal and external, designed and delivered alongside, and in support of, the crisis management function" (British Standard Institution, 2014, p. 21). Unfortunately, the SCCT mainly provides references to how crisis information is framed in the media (Nurse & Knight, 2020). Nevertheless, the focus should not be on framing, as ensuring the organization establishes its own narrative is essential, as that is what ensures the correct portray of events in the media.

A long with digitalization, communication tools have developed to increase communication methods within the cyber domain (Berg, 2017; Bakos, Dumitras, & Harangus, 2019). Not only has this increased the reach of media, it has also increased the need to successfully manage what is being communicated in case of a crisis. Communication in a cyber crisis being labeled as more complex due to the potential sensitive nature of events, newness of such situations and lacking cyber crisis communication standards. Current existing guidelines such as the SCCT create a foundational understanding, yet are argued by scholars to lack criteria pertaining to the action of how to successfully communicate (Avery, Lariscy, Kim, & Hocke, 2010; Knight & Nurse, 2020). Further, communicating cyber related crisis can be challenging due to the audience's perceived knowledge regarding cyber related incidents. Due to the complex nature of the crisis, its consequences and attribution, it may be hard to create an organization's own narrative. Establishing quick communication with external parties is of great importance as "92% of cyber security breaches were discovered by a third" (Kulikova, Heil, van den Berg, & Pieters, 2012, p. 103). Potential disinformation can result in a misperception by the public or stakeholders.

Therefore, transparency in information and communication is essential in providing the correct narrative (Backman, 2020). Transparency being an essential factor in communication within a cyber crisis, being defined by characteristics of openness and taking accountability. This being of great importance as it quickly engages stakeholders in response and has the potential to "increase overall transparency of an organization, which is beneficial for any company in times of new disclosure regulations and increased public scrutiny" (Kulikova, Heil, van den Berg, & Pieters, 2012, p. 103).

Therefore, this leads to the development of the fifth working proposition:

WP5: Transparent and clear communication with partners and stakeholders positively influence a cyber crisis response.

2.6.3. Reflective Learning

The sixth condition for effective cyber crisis management is the ability to learn from past events. If done successfully, the assessment and evaluation of how an organization responds to a cyber crisis can improve an organizations' cyber crisis resilience. Thus, by using situational output and support systems such as trainings, plans, or processes, reflective learning can be achieved (Amorim, Andler, Laere, Gustavsson, & Azevedo, 2013).

Cyber incidents and crisis have the potential to be excellent learning opportunities and a catalyst for change. The main argument for this being that the situation lends itself to thorough analysis. Learning and change opportunities arise due to the impact of the event, thus attract the attention of all stakeholders. Due to the internal and external portrayal of events, organizations feel pressured to act and implements change (Birkland, 2009). This could signify the implantation of a cyber security agenda or conducting root cause analysis. Yet, according to Birkland (2009), many documents listing lessons learned from crisis are often fantasy documents, as they generally do not touch upon the root of the causes and solutions to crisis. Such documents attempt to prove that an actor has done something about the disaster, suggesting change. Yet due to the difficulty in testing actual learning prior to cyber crisis, post-disaster documents are often neglected after publication (Birkland, 2009). Research suggests that recommendations remain inadequately implemented as cyber issues "are still not a core part of business strategy and culture" (Spremić & Šimunic, 2018, p. 344). Investments are made in technical cyber security measures, yet organizational learning remains lacking as often the individual within the organization is left behind (Carías, Labaka, María, Sarriegi, & Hernantes, 2019; Vieane, et al., 2016). Without reflective learning individuals lack the right set of tools, in turn "magnify[ing] existing weaknesses and flaws" (Danet & Weber, 2020, p. 82). Reflective learning having the potential to increase situational awareness, thus minimize the negative impact of cyber crisis on organizations (Kulikova, Heil, van den Berg, & Pieters, 2012).

Therefore, this leads to the development of the sixth working proposition:

WP6: Learning from past- cyber crisis increases the effectiveness of an organization's cyber crisis response.

2.7. Conclusion

Having understood the importance of effective cyber crisis management and the pre and post factors initiates the analysis of the influence of the factors on cyber crisis management. In doing so, the research is further conducted by analyzing two cyber security cases based on the dimensions of the working propositions discussed above. Having reasoned that cyber crisis management is influenced by pre factors, such as cyber crisis management structures, cyber program integration, as well as cooperation and information sharing, these factors are independently addressed within and across the cases. Further the post factors are examined by analyzing crisis leadership, transparent communication and reflective learning in both cases. Consequently, these influences are analyzed by conducting interviews and assessing documentary data.

3. Methodology

A multiple case study research design based on the principles of Eisenhardt (1989) and Yin (2003) will provide the basis for analysis. The following section addresses the foundations of the research, use of the qualitative multiple case study design, the sampling approach and data collection. Lastly, the approach towards data analysis is presented.

3.1. Foundations of Research

The foundations of research must be considered in order to understand and establish the grounds for investigation. The ontological and epistemological foundations are considered as they determine what is “a valid, legitimate contribution to theory” (Brannick & Coghlan, 2007, p. 62). The research ontology is considered to be objective, positivist, as it questions the nature of reality (Lincoln, Lynham, & Guba, 2011). The epistemology of research is reflected in the “nature of knowledge, what constitutes valid knowledge” (Ryan, 2006, p. 15). This is considered to be post-positivist as research is approached through a literature review establishing a framework for investigation (Brannick & Coghlan, 2007). This forms the grounds of deductive rationalization (Lincoln, Lynham, & Guba, 2011; Ryan, 2006). Consequently, following these principles this research aims to be as objective as possible, further highlighted in the structured approach in the following section.

3.2. Qualitative Multiple Case Study Research Design

The research foundation reflects the structured grounds for this study’s qualitative research. Qualitative research being one of the driving forces behind the development of theory building (Eisenhardt, 1989). Contrary to quantitative research methods qualitative studies provide greater and more in-depth insight by focusing “efforts on theoretically useful cases” (Eisenhardt, 1989, p. 533). As reflected in the positivist ontology and post-positivist epistemology theory is established through logical deduction (Lincoln, Lynham, & Guba, 2011). The deductive theoretical grounds were established as propositions were formulated based on literature, in turn allowing theory to be critically assessed and be tested. This reflects how the research seeks to understand how pre and post factors influence cyber crisis response, in order to test and contribute to literature on crisis response within the cyber domain. Building on these grounds, research is supported through a multiple case study design.

The case study research method is reflected in the study's research question, as it "focuses on understanding the dynamics present within single settings" (Eisenhardt, 1989, p. 534). This approach allows the propositions to be addressed in terms of exploring and challenging existing theory (Saunders, Lewis, & Thornhill, 2009). More specifically, a multiple case study research design is used as it allows findings to be compared and contrasted, as well as increasing the reliability of research (Baxter & Jack, 2018). Within the multiple case study research design literal replication logic is used in order to critically assess cyber crisis situations. As illustrated in the case selection section, two similar cases were purposely selected in order to establish whether theory predicts similar results. In turn, establishing the basis for an explanatory case study, as this research "aims to seek new insights, ask new questions and to assess topics in a new light" (Saunders & Lewis, 2012, p. 110). Consequently, these grounds of research are essential to understanding concepts of crisis response within cyber security.

3.3. Case Selection

The sample consists of two cyber crisis management cases that are purposely selected. The purposive sampling selection creates room for understanding of "what is happening [in order to] make logical generalizations" (Saunders & Lewis, 2012, p. 139). Following the case selection criteria are illustrated.

The two cases were selected based on the following criteria: (1) geographical location, (2) public domain, (3) mission with security elements, (4) cyber crisis, and (5) crisis response. Firstly, the organization must be established in the Netherlands as crisis response, openness of communication, as well as rules and regulations significantly differ between countries. This is due to the international data collection is too complex considering that there is no standardization in identifying cyber crisis in the EU (Čelik, 2019). Secondly, organizations must be characterized as one within the public domain, in order to ensure transparency and availability of data. Third, organizations' missions must encompass elements of a security strategy. Such being characterized by goals pertaining to establishing tools, policies and guidelines ensuring safety in the online domain (Spremić & Šimunic, 2018; ITU, 2008). Fourth, organizations must have been subject to a cyber crisis. Cyber crisis being characterized by an intangible breach within an organization's information systems, having the potential to significantly disrupt operations. Following, in order to research crisis response cases must contain elements pertaining to a crisis response. Such elements can be interpreted as the involvement of an external parties aiding in recovery or research, openly communicated data, as well as cyber security implementations. Lastly, cases between 2018 and 2020 are considered for the relevance of research due to the fast changing digital landscape. Therefore, Table 4 indicates the criteria with which the two cases have been selected. The cyber crisis management situations are selected based on the established criteria so that the influence of the pre and post factors can be assessed.

Case	Organization	Operational Location	Sector	Security Mission	Year	Cyber Crisis	Cyber Crisis Description	Crisis Response Elements
1	Maastricht University	Maastricht, the Netherlands	Public sector*	To innovate, include, ensure responsibility, encompass sustainability and share cyber security as a joint responsibility (Maastricht University, 2020).	2019	Ransomware attack**	December 23rd, 2019 Maastricht University was subject to a ransomware-attack. Data of servers was encrypted, and ransom was demanded (Fox-IT, 2020).	Crisis investigation by Fox-IT, policies concerning regular software updates, and cyber security awareness program (Maastricht University, 2020).
2	Municipality of Lochem	Lochem, the Netherlands	Public sector*	To create space for innovation, prioritizing society by modernizing (Muncipality of Lochem, 2020).	2019	Ransomware attack**	June 6th, 2019 the municipality of Lochem's ICT-system was hacked. Administrative data was encrypted, and ransom was demanded (Municipality of Lochem, 2019).	NFIR incident trace research, penetration testing, and regular system updates (Municipality of Lochem, 2019) .

Table 4: Case Overview

Source: Author

Notes:

*, The public sector being defines as; governmental and publicly organized or funded organizations.

**, Ransomware attacks being defined as; the deliberate sharing of documents or URL's that when opened activate encryption processes, consequently blocking files, users, or systems from access (Mansfield-Devine, 2016).

3.4. Data Collection

The data collection is further framed by the research design. Primary data is collected through the use of semi-structured interviews, reflecting the explanatory nature of this research (Saunders, Lewis, & Thornhill, 2009). Semi-structured interviews allow themes to be flexibly covered and give participants more freedom in expressing detailed information (Saunders & Lewis, 2012, p. 110)(Yin, 2003) (Dasgupta, 2015). Table 5 provides an overview of the semi-structured interviews, outlining themes, working propositions and the related questions. In turn, enhancing the internal validity of this research, as data is analyzed based on propositions established from theory (Dasgupta, 2015).

The primary data is further supported through the collection of information from secondary sources such as the organizations websites, newspaper articles, and shared situational reports. Through the use of multiple sources data triangulation is ensured, thus establishing construct validity as significant data is collected (Saunder & Lewis, 2012).

Consequently, after identifying two potential organizations through personal connections, participation was established. For both cases an expert is selected that was a part of the response phase within the crisis. Additionally, the experts are not part of the organizations at which the crisis occurred, in turn allowing for a stronger unbiased view on the pre and post factors in the specific crisis. Consequently, two interviews were conducted of approximately 45 minutes. The interviews were both conducted in Dutch, one by phone and one by video-call, specifically Microsoft Teams. By conducting two interviews the research aims to increase its external validity (Dasgupta, 2015). Participants were informed of the research goal and use of data. Due to the confidential nature of information within the cyber security domain the interviews were not recorded. Additionally, participants requested to remain anonymous and therefore there is only reference to the organization subject to the crisis and not the individual. Consequently, by outlining the research method and establishing protocols for data collection reliability is established. The aim of outlining the research being to show how assumptions are made and to produce consistent findings (Saunder & Lewis, 2012).

	WP1	WP2	WP3	WP4	WP5	WP6
General Information						
Could you tell me about your professional background?	-	-	-	-	-	-
Could you elaborate on your current position?	-	-	-	-	-	-
Can you specify your role and responsibilities within the cyber crisis?	-	-	-	-	-	-
Pre Factors						
What types of cyber security organizational structures were present within the organization, prior to the crisis?	x					
Could you specify what these organizational structures entailed?	x	x				
Are these organizational structures integrated throughout the whole organization?	x	x	x			
How can these organizational structures influence crisis response?	x					
How is IT structured within the organization?		x				
What type of activities define the IT organization?		x				
How would you characterize the alignment and cooperation between IT and the organization as a whole?		x	x			
To what extent data with regard to threats and risks being shared with external stakeholders?			x		x	
Post factors						
How would you characterize crisis leadership?				x		
To what extent are these characteristics present in the organization?				x		
How would you describe communication with partners and stakeholders concerning the crisis?					x	
How was critical evaluation a part of the reflection on the crisis?						x
What kind of recommendations were developed looking back the crisis?						x
To what extent have these recommendations been implemented?						x

Table 5: Matrix Interview Questions

Source: Author

Notes:

WP, indicating the working proposition

-, not applicable to the working proposition

x, relating to the noted working proposition

3.5. Data Analysis Method

Following the research design, interviews were conducted, and secondary data was collected. The interviews were not recorded, therefore notes were taken during the interviews. The notes were analyzed through the use of transcription. As illustrated in Table 6, codes were created pertaining to the propositions. Within the codes, sub-codes were established to further categorize information. This helped in identifying factors relating to the working propositions.

Code	Sub-Code	WP	Description
Pre Response	Crisis management structures	WP 1	Referring to crisis management structures such as processes, protocols, plans and training schemes.
	Business continuity	WP 1	Characteristics referring to the ability of delivering products or services without significant business disruption (British Standard Institution, 2014).
	Cyber program integration	WP 2	The adoption of cyber security within all aspects of the organization.
	Organizational Structures	WP 2	The planning, structuring and execution of activities within organizations.
	Data sharing	WP 3	Characteristics referring to the exchange of information.
	Transparency	WP 3, WP 5	Organizational elements relating to the openness with regard to communication about events.
Post Response	Crisis Leadership	WP 4	Indication of an organizations ability to coordinate, cooperate and provide guidance (Boin, Kuipers, & Overdijk, 2013, p. 81).
	Norms and Values	WP 4	Relating to norms and values reflected in the organization's roots, belief and behavior (British Standard Institution, 2014).
	Internal and External Stakeholders	WP 3, WP 5	Reference to the relation between the organization, partnerships and external parties.
	Learning and Development	WP 6	Characteristics referring to lessons learned, best practices, and testing hypotheses against reality (Boin, Kuipers, & Overdijk, 2013, p. 81).
	Resilience	WP 6	The ability to come back at a prior operational level after facing losses, reflecting flexibility and adaptation to new circumstance (Boin, Kuipers, & Overdijk, 2013, p. 81).

Table 6: Coding Scheme

Source: Author

Notes:

WP, indicating the working proposition

4. Results

The following sections introduces the results of the two cyber crisis management cases. Within this section, the cases are individually analyzed based on the themes emerging from the analysis. Thereafter, the within-cases analyses are compared, identifying and analyzing the factors influencing cyber crisis management. After discussing the factors, the section is concluded by connecting the findings to the working propositions.

4.1. Within-Case Analysis

This section aims to gain insights into the two cyber crisis management cases. By analyzing the individual cases, an explanation on the pre and post factors that influences effective cyber crisis management is established.

4.1.1. Case 1: Maastricht University

On the 23rd of December 2019, two IT security employees from Maastricht University contacted Fox-IT's alarm line, the CERT for cyber related incidents (Dantzig & Dijkstra, 2020). While the IT security employees suspected malicious activity within their network, it became clear that the attackers had already gained access to the network on the 16th of October 2019. In the 6 weeks between entering the network and being detected, the attackers managed to compromise 267 Windows servers on which they deployed the so-called Clop-ransomware (Maastricht University, 2020; Dantzig & Dijkstra, 2020).

Maastricht University counts approximately 20.000 students and 4.400 employees (Maastricht University, 2021). The university has numerous faculties and research groups that are all interconnected to the central network of Maastricht University (Maastricht University, 2021). The urgency of the availability of the network became apparent on the 23rd of December 2019, when the majority of the universities systems was encrypted, in turn halting all research and educational activities (Maastricht University, 2020).

While the university was well prepared in terms of physical security, the opposite was true regarding its cyber security maturity. Investigative reports from the Dutch ministry of education and IT security company Fox-IT shown that while cyber awareness had been a reoccurring topic on the agenda of Maastricht University, this was mostly pointed towards privacy related measures regarding the General Data Protection Regulation (GDPR) directive (Ministerie van Onderwijs, Cultuur en Wetenschap, 2020). Further, while Maastricht University had its own CERT and CISO, the reviewing of controls and measures that resulted from the IT policy was not carried out appropriately (Ministerie van Onderwijs, Cultuur en Wetenschap, 2020).

While IT controls were implemented, there no playbooks available or trainings for responding towards cyber threats (Ministerie van Onderwijs, Cultuur en Wetenschap, 2020). As a result, creating the potential for severe time loss in responding to a cyber crisis. One of the primary examples being reflected in the implementation of measures or controls that focus on backups. When not practiced, the successful retrieval of backups can be delayed, resulting in a faltering crisis response and potential data loss. Unfortunately, this happened at Maastricht University, as backups were made yet not set up right. Thus, the retrieval of backups could not be conducted (Dantzig & Dijkstra, 2020).

One of the main difficulties within the case of Maastricht University was the complexity of the network. While the network started relatively small, the increasing connections with a lack of cyber due diligence allowed the network to become increasingly complex, as well as difficult to monitor and manage (Dantzig & Dijkstra, 2020). The network had become so complex that it was difficult to have a clear overview. Resulting in the lack of segmentation, allowing the attackers to roll out the Clop-ransomware on 267 Windows servers (Dantzig & Dijkstra, 2020). Without adequate segmentation and monitoring, the scope of the ransomware attack was difficult to nearly impossible to determine. Already in the year prior to the ransomware attack, Maastricht University was in the process of implementing a Security Operations Center (SOC) with 2-3 trained operators (Cisco, 2019). Yet as education and not cyber security was its core business, the implementation had been delayed due to cost constraints (Maastricht University, 2020).

At the time of the ransomware attack, the integration of the cyber function within organization's crisis organizations in development. When Fox-IT first arrived on-site at Maastricht University, an adequate crisis organization structure had not yet been established. Communication was primary conducted with the IT department, while in times of crisis, a mandate is needed to act quickly and for the whole organization (Dantzig & Dijkstra, 2020). When a potential crisis arises quick upscaling is essential, so that all necessary decisions can be made, by those that have the right mandate within the organization. In the worst case scenario, an individual needs to be appointed whom has the position to pull the plugs, and thus halt all network activities, including that of critical business functions. Specifically, in the early phase of the ransomware attack at Maastricht University an effective response was needed so that the attackers were contained within certain parts of the network (Dantzig & Dijkstra, 2020). While the cyber security maturity and cyber program integration was low at Maastricht University, this did not resulted in an inadequate crisis response that worsened the situation (Ministerie van Onderwijs, Cultuur en Wetenschap, 2020).

Within the first moments of the ransomware attack, the IT department initiated the isolation and containment of its systems. While there were no playbooks in place, the containing of the system, instead of pulling the plugs was perceived to be an effective response (Ministerie van Onderwijs, Cultuur en Wetenschap, 2020). Yet due to of the lack of information and intangible nature that resides in cyber related threats, effective crisis leadership requires a different set of skills than when dealing with other crisis. As previously mentioned, making effective decisions with regard to cyber related incidents requires specific knowledge. In the case of Maastricht University, the IT department initially made the first effective and crucial decisions themselves. Namely, initiating he isolation and containment of systems within the network, as well as contacting Fox-IT for support. When on-scene, decision makers could follow the advice of Fox-IT, in turn establishing the formation of its crisis response organization (Dantzig & Dijkstra, 2020).

Within its crisis response, Maastricht University focused on a strategy that revolved around the idea of sharing their own bad news externally. This included the publication of an investigative report that had been drafted by Fox-IT, with their own introduction letter attached in front, explaining their view of the situation.

Inherent to a ransomware attack is the question whether one should pay ransom or not. Depending on the cruciality of the organizations and its systems that have been encrypted, organizations make a cost benefit analysis to assess their options. Whilst paying ransom is never a popular way to go, the long-term encryption of systems and data can have severe consequences. In addition, it is also not guaranteed that encrypted files will ever be restored. In the case of Maastricht University, the organization transferred 197.000 Euro’s to the cyber criminals after they received the decryption key (Heck, 2020). The payment of ransom resulted in questions from both the public as well as government, as to what extent the government actively interfered and participated in the paying of ransom (Ministerie van Justitie en Veiligheid, 2020). However, an investigative by the Ministry of Education concluded that the decision to pay ransom was the most ideal situation (Ministerie van Onderwijs, Cultuur en Wetenschap, 2020).

Specifically, in cyber security the cost benefit analysis for security investments is difficult to calculate, as the return on investment (ROI) remains unclear. However, after major incidents, cyber related developments are often prioritized. The report that was drafted by Fox-IT summarized multiple improvements for Maastricht University, with regard to its cyber resilience (Dantzig & Dijkstra, 2020). It appears that until this point, the ransomware attack was a catalyst for change that gained momentum, yet remains to be finished, as the universities cyber security awareness program still has to be improved.

Case 1: Maastricht University			
Code	**Sub-Code**	**Findings**	**Data***
Pre Response	Crisis Management Structures	There were limited policies, protocols and plans available within the organization.	"Within the university, there were no specific plans, protocols or processes in place for crisis management."
	Business Continuity	Monitoring solutions, backup retrieval and segmentation of the network were not adequately implemented.	"The size and complexity of the universities network resulted in a situation in which there was not a clear overview of the network and resulted in a lack of segmentation within the network. So, in the case an incident became apparent, there was an immediate problem because the scope was not easily to be uncovered. This was also the result of insufficient monitoring solutions."
	Cyber Program Integration	The IT department was not fully integrated within the organization's governance structure, even as the alignment of activities between IT and the rest of the organization.	"In first instance, Fox-IT officials were working together with the IT department who were not in the position to make any formal decisions."
	Organizational Structures		
	Data Sharing	There were no signs that information was shared regarding new risks and threats with partners or on information sharing platforms.	"The university did not expect to be targeted by a ransomware attack and therefore did not specifically implemented measures to deal with a cyber crisis."
	Transparency	While there was no formal communication strategy, the university choose to be transparent in its communication and to publish the investigative report that was written by Fox-IT.	"When looking at the communication coming from Maastricht University to the public, it can be stated that followed a strategy as, be the bringer of your own bad news."
Post Response	Crisis Leadership	The initial response was hectic and limited. With the assistance of Fox-IT an effective crisis response in terms of leadership and communication was established.	"When Fox-IT was called to assist with the ransomware attack, it became apparent that escalation and the formal structuring of the crisis organization did not go effectively. In first instance, Fox-IT officials were working together with the IT department who were not in the position to make any formal decisions."
	Norms and Values	The university partially acted in line with its norms in values by following a communication strategy that focused on transparency. However, it is not clear how the paying of ransom is in line with its core values.	"When looking at the communication coming from Maastricht University to the public, it can be stated that followed a strategy as, be the bringer of your own bad news'."
	Internal and External Stakeholders	There is no evidence supporting the existence of partnerships or information sharing platforms with regard to Cyber Security. There was no prior contract between Fox-IT and Maastricht University with regard to a potential cyber incident response.	"The size and complexity of the universities network resulted in a situation in which there was not a clear overview of the network and resulted in a lack of segmentation within the network."
	Learning and Development	Maastricht University requested Fox-IT to draft a report with recommendations which has been published.	"It seems that the majority of the recommendations have been followed up by the university. There is a new awareness program set up that aims to increase security awareness within the university and additional monitoring measures have been purchased and implemented."
	Resilience	The majority of the recommendations have been followed and there is currently a strong focus on cyber security and awareness within Maastricht University.	

Table 7: Results Case 1, Maastricht University

Source: Author

Notes:

*, referring to data extracted from the notes illustrated in Appendix A & B

4.1.2. Case 2: Municipality of Lochem

On Thursday the 6th of June 2019, the municipality of Lochem received a notification that there was unusual internet traffic coming from their servers. The notifier knew that the municipality of Lochem was the one creating the unusual internet traffic due to a traced IP address (De Winter, 2019). In cooperation with the National Cyber Security Centre (NCSC) and the Information Security Service for Municipalities (IBD) the Municipality of Lochem analyzed the situation, yet came to the conclusion that its systems were infiltrated (Informatiebeveiligingsdienst (IBD), 2019) (NFIR, 2019). Following, on the 7th of June the major of the municipality of Lochem decided to setup a crisis team, as well as request the assistance of an external IT- security company to investigate the incident. It was during the first meeting of the crisis team that proactive communication towards the public was established, as well as setting the intention of fully learning from the events (De Winter, 2019).

On the 12th of June research signals indicated that the attackers might have made a copy of the database with data regarding employees, including personal details such as email addresses and usernames. Unfortunately, after an initial investigation into the copying of data, it could not be excluded that the attackers were in the possession of the so called admin rights (NFIR, 2019). With that information the crisis team and the major of Lochem decided to close off the internet connection between the municipalities systems and the outside world (De Winter, 2019). As a result, all systems from the municipality could not be accessed and all business operations were halted as of the 13th of June until further notice. The following days, a new authentication server was programmed and the municipalities systems and services could slowly be restored (Municipality of Lochem, 2019).

After the initial investigation, it became apparent that the attackers gained access to the login services and that several messages were posted in which the hackers requested ransom. Besides requesting ransom, the attackers attempted to deploy malware in which they fortunately were not successful (NFIR, 2019). The initial investigation made it clear that the attackers aimed to encrypt data, demanding ransom in return for the decryption key. With the attack, no further personal identifiable information form citizens had been breached into, stolen or modified. The municipality of Lochem reported the hack to the Authority of Personal-Information (AP), the Dutch institution focusing on privacy related manners (De Winter, 2019).

The major of Lochem, who led the crisis, was increasingly transparent regarding the situation. He regarded the situation as something to be learned from, for the municipality as well as all those in similar organizational operations (Informatiebeveiligingsdienst (IBD), 2019). Transparency was something that was established from the start of the incident, positively reinforcing organizational learning and development (De Winter, 2019). Transparency was key, as in the case of local governance, citizens needed to be ensured of trust and that their personal data was safe. Therefore, according to the major of Lochem learning from this incident was key, as it improved their resilience and diminished the chance of a new future attacks (De gezonde digitale organizatie, n.d.).

Within the municipality of Lochem the IT department, its resources and organizational maturity were relatively scarce. At the time of the hack there were no plans present in the domain of information security, business continuity and crisis management (De Winter, 2019). However, due to the significant leadership of the major of Lochem, effective decision-making was possible (Informatiebeveiligingsdienst (IBD), 2019). If this had not been the case, ownership could have been transferred to the National Coordination of Terrorism and Safety (NCTV). Yet in this case, ownership in responding to the case was preferred to remain with the major of Lochem, as he carried great awareness regarding the organization, its systems and data (De gezonde digitale organizatie, n.d.).

As no action plans existed, the identification of stakeholders needed be conducted, as to whom to contact in the case of a ransomware attack. Fortunately, the major directly happened to make the right call to B. de Winter. Their professional connection and the coincidence of having worked together in a training prior to the crisis, led to the first and successful call in cyber crisis response. De Winter, a research journalist in the field of cyber security had extensive knowledge and experience in the area of cyber-attacks. After the call, he became the advisor to the major of Lochem in their crisis response (Gemeente Lochem, 2019). As can be seen in the case of the municipality of Lochem, training was essential in preparing for and acting towards the cyber related crisis. With regard to cyber crisis management, it was important to have somewhat knowledge on the basics of information technologies, in order to make critical decisions.

Communication being essential when dealing with cyber crisis. Specifically, in the case of governmental organizations, transparency becomes a defining factor in communication. As it is essential to remain trusted in the public eye, as well as that often the outcome of such cyber-attacks is often openly discussed. In the case of the Municipality of Lochem, large amounts of data were dealt with in containing and addressing the situation, as well as transparently communicating such (Gemeente Lochem, 2019) (De Winter, 2019).

In retrospect the municipality of Lochem developed plans in dealing with future cyber incidents, as well as on how to respond to other potential cyber crisis. Transparency was established, as the municipality of Lochem positioned itself as a partner for other governmental agencies in terms of cyber crisis education (Informatiebeveiligingsdienst (IBD), 2019). Unfortunately, it seems that even with the hack in Lochem, other municipalities within the Netherlands were unable to learn from others mistakes. As at the end of 2020, the Hof van Twente was hit by a ransomware attack. This organization choose to communicate that it was not the victim of a ransomware attack, yet that there was a temporary outage of their systems. While information was scarce, by following this communication strategy, the major of Hof van Twente eventually needed to explain to the media that it truly was a ransomware attack, and that she knew this from the beginning (Roetman, 2020; Herter, 2020).

Case 1: Municipality of Lochem			
Code	**Sub-Code**	**Findings**	**Data***
Pre Response	Crisis Management Structures	There were limited policies, protocols and plans available within the organization.	“While the major was known with information security and its potential risks the maturity of the organization’s cyber security was low. While there were some policies available, plans and protocols had not been implemented.”
	Business Continuity	Limited business continuity measures, plans and structures were implemented with regard to the organization’s information systems.	
	Cyber Program Integration	The IT department was not efficiently integrated within the organization’s governance structure. The roles and responsibilities for information security were not always clear.	“The organizations IT department is led by the CISO. However, it was not specifically clear for everyone what the CISO’s role was.”
	Organizational Structures		
	Data Sharing	Besides receiving occasional threat intelligence from the Dutch authorities there was no information shared regarding new risks and threats with partners or on information sharing platforms.	“Because of the size and low cyber security maturity of the organization, there had not been any alignment with other stakeholders who could, for example, assist in the case anything went wrong, or to share knowledge with”
	Transparency	While there was no formal communication strategy in place, the major of Lochem choose to be transparent in its communication and the outcomes of any investigation.	“The communication strategy that was chosen was based on transparency and. The municipality decided that it wanted to act as an example from other organizations and that they could learn from this.”
Post Response	Crisis Leadership	While there were no crisis plans available, crisis leadership and the crisis response were effective due to the professional connection between the major and cyber security expert.	“During the event, a decision had to be made for who was going the be in control. The municipality or another governmental branch. By staying in the lead, the municipality prevented that a team was making the decisions that was not aware of the internal organization within the systems of the municipality of Lochem.”
	Norms and Values	The major of Lochem focused on transparency and acting as an example or learning experience and thus aiming to improve the societies cyber resilience.	“Already in the early stages of the hack, he already made it clear that he was going to focus on transparency and learning from the situation.”
	Internal and External Stakeholders	There is no evidence supporting the existence of partnerships or information sharing platforms with regard to cyber security.	“Because of the size and low cyber security maturity of the organization, there had not been any alignment with other stakeholders who could, for example, assist in the case anything went wrong, or to share knowledge with”
	Learning and Development	A formal report has been drafted with the gaps and recommendations to prevent any incidents in the future.	“Already in the early stages of the hack, he already made it clear that he was going to focus on transparency and learning from the situation.”
	Resilience	It is not clear to what extent the recommendations or gaps have been followed up.	

Table 8: Results Case 2, Municipality of Lochem

Source: Author
Notes:
*, referring to data extracted from the notes illustrated in Appendix A & B

4.2. Cross-Case Analysis and Discussion

An essential aspect of the multiple case study design is the cross-case analysis. Having understood and analyzed both cases separately, patterns and similarities between the two cases can be assessed. In turn, leading to the integration of the discussion of the findings and allowing the analysis to be concluded by relating the findings to the working propositions of the theoretical framework.

4.2.1. Pre Factors

In assessing the pre factors crucial to cyber crisis management and reflected in Table 9, it has been become apparent that planning for cyber related crisis is essential for effective response and key to minimizing negative effects (Berg, 2017). The analysis has indicated that both organizations did not establish adequate cyber crisis management structures prior to the cyber-attacks. Within the crisis management structures, crisis management and business continuity plans, measures, policies, processes or protocols were inadequately integrated. The absence of such resulted in an unstructured initial crisis response, in which the roles and responsibilities were not consistently clear for all stakeholders (British Standard Institution, 2014). Specifically, in the case of Maastricht University's, core business operations consisting of education and research were practically completely halted. Measures regarding business continuity such as the retrieval of backups, network monitoring and network segmentation were not implemented well enough to prevent or mitigate the negative cyber-attack effects. In turn, acknowledging the need for effective business continuity and cyber crisis management structures that include training in turn establishing greater awareness amongst all stakeholders (Backman, 2020).

Second, there is a need for internal efficiency in order to respond quickly and effectively through successful cyber program integration. In analyzing both cases, it became apparent that the IT departments were not fully integrated into the organizational structures. This resulted in time losses, regarding detection as well as response. More specifically, when Fox-IT officials arrived on site at Maastricht University, no CMT established. The event remained to be dealt with by just the IT department. While there is an increasing understanding of the importance in addressing cyber risk, there is still lacking motivation and gaps within the realization on how to fully integrate cyber programs within governance models, in turn resulting in inefficiencies when responding to cyber incidents or crisis (Thycotic, 2019).

Third, the sharing of data regarding new risks and threats is vital for any organization to keep track of developments in cyberspace. Therefore, the changing cyber threat landscape and the continuous interconnection and aggregation of organizations requires greater coordination in mitigating risks (KPN et. al., 2020). In both cases, there was no evidence of pro-active cooperation and information sharing with cooperating parties, platforms or with regulators.

Fourth, while both cases had no pre-defined communication strategy, both organizations choose to be transparent in their communication towards the public and its stakeholders. Transparency was accomplished both during the event, as well as in the aftermath by publishing reports that included root cause analysis and recommendations. While often difficult to achieve, the quick transfer of correct information to the public and gaining control of the narrative remains vital in managing cyber crisis effectively (Backman, 2020). Moreover, by not communicating effectively during a crisis, “more damages [can be caused] than [by] the crisis itself” (Bakos, Dumitras, & Harangus, 2019, p. 2). In both situations, the communication strategy positively influenced the crisis response, thus resulted in control of the narrative. This finding was thoroughly supported through Maastricht University’s publishing of external reports that included root cause analysis and recommendations for future improvement. These reports were published by the university and even included a cover letter with the university’s perspective.

Code	Sub-Code	Findings	Case 1: Maastricht University	Case 2: Municipality of Lochem
Pre Response	Crisis Management Structures	Both organizations did not have adequate crisis management structures such as a crisis management plans, processes or protocols.	There were limited policies, protocols and plans available within the organization.	There were limited policies, protocols and plans available within the organization.
	Business Continuity	In both cases the business continuity plans, measures, processes or protocols were inadequate or effective in preparing for and responding to a ransomware attack.	Monitoring solutions, backup retrieval and segmentation of the network were not adequately implemented.	Limited business continuity measures, plans and structures were implemented with regard to the organization’s information systems.
	Cyber Program Integration	In both cases the IT department was not fully or efficiently integrated within the organization’s governance structure.	The IT department was not fully integrated within the organization’s governance structure, just as the alignment of activities between IT and the rest of the organization.	The IT department was not efficiently integrated within the organization’s governance structure. The roles and responsibilities for information security were not always clear.
	Organizational Structures			
	Data Sharing	Both organizations did not actively engage in information sharing partnerships or platforms to gain knowledge on new risks and threats.	There were no signs that information was shared regarding new risks and threats with partners or on information sharing platforms.	Besides receiving occasional threat intelligence from the Dutch authorities there was no information shared regarding new risks and threats with partners or on information sharing platforms.
	Transparency	In both cases the organization choose to follow a strategy of transparency in its communication to stakeholders and the public.	While there was no formal communication strategy, the university choose to be transparent in its communication and to publish the investigative report that was written by Fox-IT.	While there was no formal communication strategy in place, the major of Lochem choose to be transparent in its communication and the outcomes of any investigation.

Table 9: Pre Factor Results of the Cross-Case Analysis

Source: Author

4.2.2. Post Factors

Whereas the pre factors focused on the preparatory activities, the post factors are characterized by elements in the aftermath of a cyber crisis. The further analysis of the post factors is depicted in Table 10. The analysis continues to indicate that in the case of crisis leadership, both organizations were required to respond to a ransomware attack. As with any other crisis response, crisis leadership has the ability to significantly establish change and when successful, has the potential to minimize negative effects of a crisis. However, if not done correctly forms of leadership may worsen the situational outcomes (Gigliotti, 2016). In line with the research's expectation, the absence of adequate cyber crisis management structures resulted in an unstructured initial crisis response. However, contrary to the research's expectations, in the case of the Municipality of Lochem, the major responded by directly contacting a professional in IT security. This expert had extensive knowledge regarding responding to ransomware attacks. While a structured process and predefined emergency contacts and contract could have positively influenced the organization's crisis leadership effectiveness, these personal relations resulted in an effective and transparent initial response. In the case of Maastricht University, the initial crisis response started unstructured. While there were no predefined emergency contacts or plans, members of the university's IT department contacted Fox-IT for assistance. With the help and advice of Fox-IT the crisis response could be structured and gained effectiveness.

Second, with regard to taking the organization's norms and values into, in both cases it became apparent that they followed a communication strategy focused on transparency. In the case of Maastricht University, this strategy was in line with one of the core elements of its mission, namely social responsibility. Nevertheless, it remains difficult to assess norms and values, due to the payment of ransom. Some would argue a negative outcome, yet other positive as there appeared to be no other way out. With regard to the Municipality of Lochem it can be stated that the major was focused on transparency, reflecting on how society as a whole could learn from this particular event. Being a governmental organization, the focus on learning within its crisis response was most certainly in line with its norms and values.

Third, in both cases there was no evidence that supported the existence of partnerships or information sharing platforms with regard to cyber security. More specifically, there were no official links or partnerships with regard to incident response or the sharing or receiving of threat intelligence.

Fourth, the learning from past events is essential to further develop an organization crisis management capability. If done successful, the assessment and evaluation of how an organization responds to a cyber crisis can improve an organizations' cyber crisis resilience. Thus, by using situational output and support systems such as trainings, plans, or processes, reflective learning can be achieved (Amorim, Andler, Laere, Gustavsson, & Azevedo, 2013). The ransomware attacks on Maastricht University and the Municipality of Lochem have proven to be excellent learning opportunities due to the impact and attention that it received from both the public as its stakeholders. In line with the research's expectations, in both cases the organizations felt the need to establish investigative reports, that included root cause analysis and recommendations aiming improve the organizations' maturity level (Birkland, 2009). However, while the analysis suggests that the lessons learned have been partially followed up at Maastricht University, it is not clear whether the topic of cyber security is still high on the agenda's or that the publications can be considered fictional documents, that in turn have not increased the organizations cyber crisis resilience (Birkland, 2009).

Code	Sub-Code	Findings	Case 1: Maastricht University	Case 2: Municipality of Lochem
Post Response	Crisis Leadership	In both cases the crisis response initiated unstructured. With the assistance of external parties, the response became structured, and crisis leadership was formed by focusing on transparency and learning.	The initial response was hectic and limited. With the assistance of Fox-IT an effective crisis response in terms of leadership and communication was established.	While there were no crisis plans available, crisis leadership and crisis response were effective due to personal connections with a cyber security expert.
	Norms and Values	In both cases the openness and transparency in its crisis communication was in line with its core values and as being part of the society.	The university partially acted in line with its norms in values by following a communication strategy that focused on transparency. Yet, it is not clear how the paying of a ransom is in line with core values.	The major of Lochem focused on transparency and acting as an example or learning experience and thus aiming to improve the societies cyber resilience.
	Internal and External Stakeholders	There is no evidence supporting the existence of partnerships or information sharing platforms with regard to cyber security.	There is no evidence supporting the existence of partnerships or information sharing platforms with regard to cyber security. Further, there was no prior contract between Fox-IT and Maastricht University with regard to a potential cyber incident response.	There is no evidence supporting the existence of partnerships or information sharing platforms with regard to cyber security.
	Learning and Development	In both cases a report was drafted to address the origin of the ransomware attack, with implications, gaps and future recommendations.	Maastricht University requested Fox-IT to draft a report with recommendations which has been published.	A formal report has been drafted with the gaps and recommendations to prevent any incidents in the future.
	Resilience	In the case of Maastricht University, it is clear that the majority of the recommendations have been followed up. For the Municipality of Lochem this is not vivid as there is no supporting evidence in this case.	The majority of the recommendations has been followed up and there is currently a strong focus on cyber security and awareness within Maastricht University.	It is not clear to what extent the recommendations or gaps have been followed up.

Table 10: Post Factor Results Cross-Case of the Analysis

Source: Author

4.2.3. Working Proposition Results

By further taking the cross- case analysis into account, the findings can be related to the working propositions as depicted in Table 11. The findings partially support WP1 as both cases did indeed have immature cyber security organizational structures. However, based on the findings it can be stated that specifically in the case of Maastricht University, a higher maturity would have provided a more complete picture in terms of monitoring and segmentation which would have made it easier to respond to the crisis. Additionally, WP2 is supported as in both cases the lack of integration and alignment of the activities between IT and the management resulted in a delay in the initial crisis response. Further, the findings partially support WP3, as there was no evidence for pro-active cooperation and information sharing with partners or stakeholders with regard to developments in the cyber risk landscape. However, in the case of the Municipality of Lochem, the swift cooperation with an IT Expert proved to be of much help. A formal cooperation and participation in for example information sharing platforms could have further assisted in identifying the risks for both organizations.

WP4 lends support from the analysis of both cases and stresses the importance of leadership that has to right knowledge and skillset to deal with the crisis at hand. Moreover, if those in charge do not possess the right knowledge, supporting functions are needed to inform and advise the leadership for making effective decisions. Further, the findings support WP5 and the analysis of both cases make it apparent that especially in cyber crisis, transparency in communication to the public and stakeholders positively influences a cyber crisis management response. Finally, the analysis of both cases partially supports WP6. As there have not been any other cyber crisis or major incidents at both organizations, there is no data that suggests that learning from a past cyber crisis did contributed to a more effective cyber crisis management response. However, the following up of recommendations, such as in the case of Maastricht University, partially supports the fact that learning from past cyber crisis can indeed increase the effectiveness of an organization’s cyber crisis response.

WP	Description	Results
1	WP 1: Immature cyber security organizational structures negatively influence cyber crisis response.	Partially Supported
2	WP 2: The integration and alignment of the activities of the CMT, CISO office, SOC and CERT will improve an organization’s cyber crisis response.	Supported
3	WP 3: A focus on pro-active cooperation and information sharing with partners and stakeholders will improve an organization’s cyber crisis response.	Partially Supported
4	WP 4: Untrained crisis leaders have a negative influence on a cyber crisis response.	Supported
5	WP 5: Transparent and clear communication with partners and stakeholders positively influence a cyber crisis response.	Supported
6	WP 6: Learning from past- cyber crisis increases the effectiveness of an organization’s cyber crisis response.	Partially Supported

Table 1: Overview of the Working Proposition Results

Source: Author

5. Conclusion

This research aimed to urge the importance of cyber security integration into crisis management programs. The research question was answered by breaking domain the BSI framework and SCCT, critically assessing the formation of pre and post cyber crisis management. By integrating the cyber security domain research gaps were identified and analyzed. In turn allowing the more detailed investigation of preparatory pre factors, as well as post response and recovery.

The pre and post factors influencing cyber crisis management were examined through a qualitative multiple case study research design. By purposively sampling two cases, data collection and analysis was achieved through conducting semi-structured interviews and collecting documentary data. Consequently, the exploratory nature of the research design allowed the research question to be answered.

The pre factor of management, preparation was assumed to be constrained due to immature cyber security organizational structures. This was partially supported as both organizations were characterized by immature structures, yet research did indicate that if plans and trainings were integrated, negative consequences could have been better mitigated. Further, support was found regarding the higher level integration of cyber programs positively influencing cyber crisis response. This was reflected in the lack of cyber security integration throughout the organizations as expertise remained within the IT departments. Lastly within the pre phase cooperation and information sharing was predicted to positively influence the outcome. Partial support was established due to lacking evidence in one case, yet a personal information sharing partner in the other case.

Furthermore, the post factor of management was characterized by response and recovery. Within the response phase untrained cyber crisis leaders were predicted to negatively influence management outcomes. Additionally, response was characterized by transparency regarding communication assessed to positively influence outcomes. Both notions were supported, as in both cases external parties enabled the establishment of successful cyber crisis leadership, as well as transparency in communication. Moreover, learning within the recovery phase was predicted to positively influence managerial actions. Yet, this notion was partially supported as investigation of implemented learning practices was limited, however the publishing of lessons learned suggest otherwise.

Consequently, in cyber crisis management it is essential that the basis or foundation of an organizations' crisis management capabilities are examined. This research examined the influence of pre and post factors and thus attempted to further integrate cyber security in the crisis management domain. By analyzing the factors that influence cyber crisis management new insights were gained into the importance of cyber security integration in current literature and research. Therefore, this research contributed through highlighting the fragmentation of and possibilities within current research, thus providing a basis for research future research opportunities.

5.1. Recommendations

The dynamic and intangible nature of cyber risks require a cyber specific focus within organization crisis management programs. Essential in dealing with cyber crisis are adequate steps in setting the stage for preparing, responding and recovering from cyber crisis. Therefore, recommendations can be derived from this research, as the pre and post factors influencing cyber crisis responses are essential. Specifically, key to cyber resilience is the integration of cyber programs in higher organizational levels, by establishing urgency for the cyber security this has the potential to become a strategic priority. Additionally, it is recommended that leadership within cyber crisis management is trained as adequate knowledge of the cyber domain is key. This further reflects the importance of transparent communication, as stakeholders can provide significant support and external perception may influence crisis outcome. Consequently, this research further encourages the investigation of crisis management within the cyber domain.

5.2. Limitations

Addressing the limitations of this research allows suggested for future research to be established. The interviews should have incorporated more questions as well as a structured interview protocol. This was not possible due to the duration of the research and the need for confidentiality to ensure participation. This relates to the limitation of unwillingness to participate. Due to the sensitive nature of crisis management limited organizations were willing to contribute to this research. By increasing the duration and scope of research, research could be expanded to provide even more detailed insight into the pre and post factors. Further, limitations lie in the nature of response to the interview questions as there is potential for bias considering the interviewees' positions held within the organizations. This can again be improved by increasing the duration and data collection sample, allowing multiple individuals to partake and providing greater insight and analysis of each case study. Additionally, the influence of pre and post factors may not be fully expressed due to the focus on ransomware attacks. Research can be expanded by including organizations that were subject to different types of cybercrime, such as hacks and Distributed Denial of Service (DDoS). Lastly, the openness of public institutions ensured greater availability of information. Yet future research samples should be expanded to fully reflect cybercrime in both public and private organizations. Therefore, these limitations provide insight into the numerous opportunities of research of crisis response within the cyber security domain.

6. Bibliography

Čelik, P. (2019). Institutional Measures for Increasing the Cyber Security for Business in the European Union. *Economic Themes, 57*(3), 351-364.

Abelson, M., & Kopechi, D. (2012, 05 26). *JPMorgan Gave Risk Oversight to Museum Head With AIG Role*. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2012-05-25/jpmorgan-gave-risk-oversight-to-museum-head-who-sat-on-aig-board

Amorim, J., Andler, S., Laere, J. v., Gustavsson, P. M., & Azevedo, A. T. (2013). Cyber Crisis Management: Applying Agile Methods for Training Development and its Implementation. *National Symposium on Technology and Methodology for Security and Crisis Management* (pp. 1-2). Krista, Sweden: Researchgate.

Avery, E., Lariscy, R., Kim, S., & Hocke, T. (2010). A quantitative review of crisis communication research in public relations from 1991 to 2009. *Public Relations Review*, 190-192.

Backman, S. (2020). Conceptualizing cyber crisis. *Contingencies and crisis managemeent*, 1-10.

Bakos, L., Dumitras, D., & Harangus, K. (2019). Human Factor Preparedness for Decentralized Crisis Management and Communication in Cyber-Physical Systems. *Sustainability*, 1-19.

Barefoot, K., Curtis, D., Jolliff, W., Nicholson, J. R., & Omohundro, R. (2018, 03 15). *Defining and Measuring the Digital Economy*. Retrieved from Bureau of Economic Analysis: https://www.bea.gov/sites/default/files/papers/defining-and-measuring-the-digital-economy.pdf

Baxter, P., & Jack, S. (2018). Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. *The Qualitative Report*, 544-556.

Berg, J. v. (2017). *Cyber Security for Everyone.* Islamorada, FL, USA: New Security Paradigms Workshop.

Birkland, T. A. (2009). Disasters, Lessons Learned, and Fantasy Documents. *Journal of Contingencies and Crisis Management*, 146-157.

Boeke, S. (2017). National cyber crisis management: Different European approaches. *Wiley Governance*, 1-17.

Boiko, A., Shendryk, V., & Boiko, O. (2019). Information systems for supply chain management: uncertainties, risks and cyber security. *Procedia Computer Science 149*, 65-70.

Boin, A., Hart, P. t., Stern, E., & Sundelius, B. (2017). *The politics of crissi management: Public leadership under pressure.* Cambridge: Cambridge University Press.

Boin, A., Kuipers, S., & Overdijk, W. (2013). Leadership in times of crisis: A framework for assessment. *International review of public administration*, 79-91.

Bonnet, D., Ferraris, P., Westerman, G., & McAfee, A. (2012). Talking ’bout a Revolution. *Digital Transformation Review, 2*(1), 17-33.

Brannick, T., & Coghlan, D. (2007). In defense of being “native”: The case for insider academic research. *Organizational research methods*, 59-74.

Brannick, T., & Coghlan, D. (2007). *In Defense of Being “Native”: The Case for Insider Academic Research* . Sage Journals.

British Standard Institution. (2014). *Crisis Management - Guidance and good practice.* Londen: BSI.

Bundy, J., Pfarrer, M., Short, C., & Coombs, T. (2017). Crisis and Crisis Management: Integration, interpretation, and research development. *Journal of Management*, 1661-1692.

Calvin, N. (2019). Establishing Human Factors Programs to Mitigate Blind Spots in Cybersecurity. *Proceedings of the Fourteenth Midwest Association for Information Systems Conference*.

Carías, J. F., Labaka, L., María, J., Sarriegi, J. M., & Hernantes, J. (2019). Defining a Cyber Resilience Investment Strategy in an Industrial Internet of Things Context. *Sensors*.

Chandini, M. S. (2020). An overview about a milestone in Information Security: Steganography. *International Journal of Progressive Research in Science and Engineering*, 33-35.

Chang, F., Dybes, S., & Moore, T. (2015). *Identifying how firms manage cybersecurity investment.* Dallas: Darwin Deason Institute for Cyber Security.

Cisco. (2019). *Cusci case study: Maastricht University.* Maastricht: Cisco.

Coombs, T. (2007). Protecting Organization Reputations During a Crisis: The Development and Application of Situational Crisis Communication Theory. *Corporate Reputation Review*, 163-167.

Coombs, T. (2008). The protective powers of crisis response strategies. *Journal of Promotion Management*, 241-260.

Danet, D., & Weber, C. (2020). Cyber Crisis Management and Leadership. *n ECCWS 2020 20th European Conference on Cyber Warfare and Security.* Academic Conferences and publishing limited.

Dantzig, M. v., & Dijkstra, M. (2020). *Spoedondersteuning Project Fontana.* Delft: Fox-IT.

Dasgupta, M. (2015). Exploring the relevance of case study research. *Vision*, 147-160.

De gezonde digitale organizatie. (n.d.). *ICT-systeem Gemeente Lochum gehackt*. Retrieved from De gezonde digitale organisatie: https://degezondedigitaleorganisatie.nl/ict-systeem-gemeente-lochem-gehackt/

De Winter, B. (2019). *Door het oog van de naald: Analyse van het beveiligingsincident in Lochem.* Lochem: Gemeente Lochem.

Eisenhardt, K. (1989). *Building theories from case study research.* Academy of Management Review.

Fox-IT. (2020). *Reactie Universiteit Maastricht op rapport FOX-IT.*

Gemeente Lochem. (2019). *Door het oog van de naald: Analyse van het beveiligingsincident in Lochem.* Lochem: Gemeente Lochem.

Gemeente Lochem. (2019, 09 5). *Gemeente Lochem door het oog van de naald bij hack* . Retrieved from Lochem: https://www.lochem.nl/laatste-nieuws/nieuwsbericht/gemeentenieuws/gemeente-lochem-door-het-oog-van-de-naald-bij-hack-2553

Giat, Y., & Dreyfuss, M. (2020). *Optimizing Data and New Methods for Efficient Knowledge Discovery and Information Resources Management.* Jerusalem: Jerusalem College of Technology.

Gigliotti, R. A. (2016). Leader as performer; leader as human: A discursive and retropective construction of crisis leadership. *Atlantic Journal of Communication*, 185-200.

Golandsky, Y. (2016). Cyber crisis management, survival or extinction? *International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* , 1-14.

Grill, B., Bacs, A., Platzer, C., & Bos, H. (2015). *"Nice Boots!" - A Large-Scale Analysis of Bootkits and New Ways to Stop Them.* Online: Springer.

Heck, W. (2020, 02 05). *Universiteit Maastricht betaalde bijna 200.000 euro losgeld*. Retrieved from NRC: https://www.nrc.nl/nieuws/2020/02/05/universiteit-maastricht-betaalde-bijna-200-000-euro-losgeld-na-ransomware-aanval-a3989357

Herter, A. (2020, 12 07). *'Hackers gemeente Hof van Twente eisen 750.000 euro losgeld'*. Retrieved from NRC.nl: https://www.nrc.nl/nieuws/2020/12/07/hackers-gemeente-hof-van-twente-eisen-750-000-euro-losgeld-a4022843

Huang, K., Siegel, M., & Madnick, S. (2018). Systematically Understanding the Cyber Attack Business: A Surevey. *ACM Computing Surveys*, 1-36.

Informatiebeveiligingsdienst (IBD). (2019). *Beschouwing incidentmanagement gemeente Lochem.* Lochem: Informatiebeveiligingsdienst (IBD).

Informatiebeveiligingsdienst (IBD). (2019). *Leren van Lochem: Lessen uit een informatiebeveiligingsincident.* Lochem: Informatiebeveiligingsdienst (IBD).

International standard for standardization. (2012). *Business continuity management systems - Requirements (ISO 22301:2012.* International standard for standardization.

International Standard Organisation. (2012). *ISO 22301: Societal Security - Business Continuity management Systems.* Geneva: International Standard Organisation.

International Standard Organisation. (2018). *ISO 31000 Risk Management.* Geneva: International Standard Organisation.

ITU. (2008). *International Telecommunications Union*. Retrieved from Definition of Cyber Security: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

Jai, T.-M., & Chen, H. (2019). Cyber Alarm: Determining the impacts of hotel's data breach messages. *International Journal of Hospitality Management*, 326-334.

Klimburg, A., & Mirtl, P. (2012). Cyberspace and governance - A Primer. *Austrian Institute for International Affairs*, 1-27.

Knight, R., & Nurse, J. (2020). A framework for effective corporate communication after cyber security incidents. *omputers & Security*.

Kolini, F. (2017). Clustering and Topic Modelling: A New Approach for Analysis of National Cyber Security Strategies. *Pacific Asia COnference on Information Systems*, 1-12.

KPN et. al. (2020). *European Cyber Security Perspectives 2019.* Amsterdam: KPN.

Kulikova, O., Heil, R., van den Berg, J., & Pieters, W. (2012). Cyber Crisis Management: A decision-support framework for disclosing security incident information. *International conference on cyber security* (pp. 103-112). IEEE.

Lee, J. (2018, May). Making cyber-security a strategic business priority. *Network Security*(5), 6-8.

Lewis, J. (2018). *Economic Impact of Cybercrime - No Slowing Down.* Santa Clara: McAfee.

Lincoln, Y., Lynham, S., & Guba, E. (2011). Paradigmatic Controversies, Contradictions, and Emerging Confluences, Revisited. In *The Sage Handbook of Qualitative Research* (pp. 97-128).

Long, R. (2017, 03 14). *BIA and Risk Assessment: Why Both Are Important*. Retrieved from MHA Consulting: https://www.mha-it.com/2017/03/14/bia-and-risk-assesment/

Maastricht University. (2020). *Cyber Security: A joint responsibility*. Retrieved from Maastricht University: https://www.maastrichtuniversity.nl/about-um/cyber-security-joint-responsibility

Maastricht University. (2020). *Cyber security: A joint responsibility!* Retrieved from Maastricht University: https://www.maastrichtuniversity.nl/about-um/cyber-security-joint-responsibility

Maastricht University. (2020). *Response of Maastricht University to FOX-IT report.* Maastricht: Maastricht University.

Maastricht University. (2021, 02 2). *About UM*. Retrieved from Maastricht University: https://www.maastrichtuniversity.nl/about-um

Mansfield-devine, S. (2016). Ransomware: taking businesses hostage. *Network Security*, 8-17.

McKinsey & Company. (2019, March). *Perspectives on transforming cybersecurity.* Retrieved from McKinsey.com: https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx

Ministerie van Justitie en Veiligheid. (2020). *Antwoorden kamervragen over de berichten 'Universiteit Maastricht betaalde hackers losgeld' en 'Verzekeraars zorgen voor toename van ransomware-aanvallen'.* Den Haag: Ministerie van Justitie en Veiligheid.

Ministerie van Onderwijs, Cultuur en Wetenschap. (2020). *Cyberaanval Universiteit Maastricht.* Utrecht: Ministerie van Onderwijs, Cultuur en Wetenschap.

Mueller, R. (2012). FBI Director.

Muncipality of Lochem. (2020). *Werken bij de gemeente Lochem*. Retrieved from Gemeente Lochem: https://www.lochem.nl/bestuur-en-organisatie/werken-bij-de-gemeente-lochem

Municipality of Lochem. (2019, 6 6). *Gemeente Lochem door het oog van de naald bij hack.* Retrieved from Gemeente Lochem: https://www.lochem.nl/laatste-nieuws/nieuwsbericht/gemeentenieuws/gemeente-lochem-door-het-oog-van-de-naald-bij-hack-2553

Nappo, S. (2019). CISO of the Week, Stéphane Nappo, Société Générale.

NCSC. (2020, 12 09). *Intensievere informatie-uitwisseling NCSC en Nederlandse cybersecuritybedrijven* . Retrieved from NCSC: https://www.ncsc.nl/actueel/nieuws/2020/december/9/intensievere-informatie-uitwisseling-ncsc-en-nederlandse-cybersecuritybedrijven

NFIR. (2019). *Managementsamenvatting Security Incident Lochem.* The Hague: NFIR: IT Forensics & Incident Response.

Niekerk, J., & Solms, R. v. (2013). From information security to cyber security. *Computers & Security*, 97-102.

Nobles, C. (2018). Botching Human Factors in Cybersecurity in Business Organizations. *HOLISTICA - Journal of Business and Public Administration, 9*(3), 71-88.

Nolan, C., Lawyer, G., & Dodd, R. M. (2019). Cybersecurity: today's most pressing governance issue. *Journal of Cyber Policy*, 425-441.

Nurse, J., & Knight, R. (2020). A framework for effective corporate communication after cyber security incidents. *Computers & Security*, 1-18.

Purse, R., Thibault, N. D., & Craigen, D. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, 13-21.

Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M., & Peersman, C. (2018). Scoping the Cyber Security Body of Knowledge. *IEEE Security and Privacy, 16*(3), 96-102.

Roetman, B. (2020, 12 07). *De gemeente Hof van Twente is digitaal gegijzeld. Moet zij over de brug komen met 750.000 euro losgeld?* Retrieved from Trouw: https://www.trouw.nl/binnenland/de-gemeente-hof-van-twente-is-digitaal-gegijzeld-moet-zij-over-de-brug-komen-met-750-000-euro-losgeld~b8be228d/?referrer=https%3A%2F%2Fwww.google.com%2F

Ryan, A. (2006). Researching and Writing your Thesis: a guide for postgraduate students. *Post-positivist approaches to research*, 12-26.

SANS. (2020, 11 17). *Information Security Resources*. Retrieved 11 17, 2020, from Sans.org: https://www.sans.org/information-security

Saunder, M., & Lewis, P. (2012). *Doing research in business & management.* Essex, UK: Pearson Education Limited.

Saunders, M., & Lewis, P. (2012). *Doing Research in Business & Management. An Essenial Guide to Planning Your Project.* Pearson.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students.* Pearson Education.

Shaheer, N. A., & Li, S. (2020). The CAGE around cyberspace? How digital innovations internationalize in a virtual world. *Journal of Business Venturing, 3*(35).

Shukla, S., & Nagurney, A. (2016). Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability. *European Journal of Operational Research*, 588-600.

Spremić, M. (2017). Governing Digital Technology – how Mature IT Governance can help in Digital Transformation? *International Journal of Economics and Management Systems, 2*, 214-223.

Spremić, M., & Šimunic, A. (2018). Cyber Security Challenges in Digital Economy. *Proceedings of the World Congress on Engineering , 1*.

Thycotic. (2019). *The CISO Challenge: Aligning Business Enablement with enforcement.* Londen: Thycotic.

UK Department for Digital, Culture, Media & Sport. (2019). *FTSE 350 Cyber Governance Health Check 2018.* London: UK Department for Digital, Culture, Media & Sport.

Vieane, A., Funke, G., Gutzwiller, R., Mancuso, V., Sawyer, B., & Wickens, C. (2016). Addressing Human Factors Gaps in Cyber Defense. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 60*(1), 770-773.

Vitunskaite, M., He, Y., Brandstetter, T., & Janicke, H. (2019). Smart cities and cyber security: Are we there yet? A comperative study on the role of standards, third party risk management and security ownership. *Computers & Security*, 313-331.

Wang, L., Wang, J., & Gwebu, K. (2018). *The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management.* Journal of Management Information Systems.

Wang, P., & Park, S.-A. (2017). Communication in Cybersecurity: A Public communication model for business data breach incident handling. *Information Systems*, 136-147.

Wirfs, J., & Eling, M. (2019). What are the actual costs of cyber risk events? *European journal of operational research*, 1109-1119.

World Economic Forum. (2019). *The Global Risks Report 2019.* Geneva: World Economic Forum.

Yin, R. (2003). *Case study research: Design and methods.* Sage Publications Inc.

Zhang, A., Collins, R., & Connor-Close, C. (2020). *Cyber incident cost estimates and the importance of building resilience.* Wellington: Reserve Bank of New Zealand.

Zhang, H., Han, W., Lai, X., LIN, D., Ma, J., & Li, J. (2015). Survey on cyberspace security. *Science China Information Sciences, 58*.

7. Appendices

7.1. Appendix A: Interview Maastricht University

Phase	Description
Introduction	The difference between regular and cyber crisis management resides in the fact that organizations usually have implemented physical security measures, yet not really in the domain of cyber security. For example, while there might are processes in place, these are not regularly practiced. By not practicing the processes, there is a significant time loss with for example the restoring of backups. While assurance standards look whether there are processes and protocols in place, these do not specifically assess and guarantee whether these are also practiced. Especially in the case of a ransomware attack, the practicing of restoring backups is essential. If not practiced right, there is a larger possibility that the backups cannot be restored in a timely matter.
Pre Factors	There is a major difference in the factual documentation of how something is working and how it works in practice. This is often overlooked and was also the case at Maastricht University. More specifically, at Maastricht University there were backups, yet these had not been set up right. In doing so, the backups could not be restored properly. One of the aspects that contributed to the not working backups was the fact that an adequate cyber due diligence was not followed during the past decades in which the university grew and multiple new networks from for example research institutes were integrated into the network of Maastricht University. Therefore, even when the main entity or organization has its systems well secured and organized, also the maturity of the purchased or cooperating parties are of importance. The size and complexity of the universities network resulted in a situation in which there was not a clear overview of the network and resulted in a lack of segmentation within the network. So, in the case an incident became apparent, there was an immediate problem because the scope was not easily to be uncovered. This was also the result of insufficient monitoring solutions. Within the university, there were no specific plans, protocols or processes in place for crisis management. Prior to the ransomware attack, the university was already in the process of implementing a SOC which was not finished yet. The university did not expect to be targeted by a ransomware attack and therefore did not specifically implemented measures to deal with a cyber crisis.
Post Factors	When Fox-IT was called to assist with the ransomware attack, it became apparent that escalation and the formal structuring of the crisis organization did not went effectively. In first instance, Fox-IT officials were working together with the IT department who were not in the position to make any formal decisions. In the case of a cyber crisis such as a ransomware attack, there needs to be a formal escalation process that can be followed. This needs to include people or roles that have the mandate to make

	decisions so that in the worst case, you can decide to ‘pull the plugs’. In the case of Maastricht University there was no formal crisis plan and therefore it was not clear who should participate in the crisis team that should respond to the ransomware attack. Together, Fox-IT and Maastricht University established a crisis team that included the representatives from communication, HR, IT, Security and a person with the mandate to make decisions. Especially in the first phases of a ransomware attack it is easiest to contain the threat. In the case of Maastricht University this was unfortunately not the case that they were forced to call the emergency phone number of Fox-IT. Maastricht University did not think that they would be the target of an attack due to the fact that they are a university and research institute. In doing so, there was no specific need for cyber crisis specific plans, protocols and policies. Due to the complexity of the matter and the fact that there was no specific cyber related knowledge within the leadership of Maastricht University, they were not prepared to take effective decisions. Therefore, Fox-IT was asked to assist in researching the attack and also to assist in the response. What went right was the fact that IT officials of Maastricht University already started to contain the networks before the Fox-IT officials arrived. In addition, when looking at the communication coming from Maastricht University to the public, it can be stated that followed a strategy as, be the bringer of your own bad news. Particularly in cyber crisis it is important for an organization to have the lead in providing news of information to the public. In the aftermath of the ransomware, Maastricht University had asked Fox-IT to assess the situation and formulate a report with lessons learned. The report that was published entailed information on how the attack has occurred and formulated recommendation that needed to be implemented to improve the universities cyber security maturity. The report was published together with a cover letter from Maastricht University with their side of the story, also in line with the communication strategy focusing on, be the bringer of your own bad news. It seems that the majority of the recommendations have been followed up by the university. There is a new awareness program set up that aims to increase security awareness within the university and additional monitoring measures have been purchased and implemented.

Table 12: Maastricht University Interview

Date: 3rd of December 2020 (16:00 – 17:00)

Source: Author

7.2. Appendix B: Interview Municipality of Lochem

Phase	Description
Introduction	Around 10 PM in the evening on the 6th of June 2019, the major of the municipality of Lochem received a phone call from its CISO who was called by the Dutch police with information that there was suspicious activity coming from their servers. Initially, the major of Lochem suspected it to be a misunderstanding as there has been a preventive test just a few days prior to the call. After also haven given a call to B. de Winter, who was involved with the test, it quickly became apparent that the threat was real. Already in the early stages of the hack, the major of Lochem already made it clear that he was going to focus on transparency and learning from the situation.
Pre Factors	While the major was known with information security and its potential risks the maturity of the organization's cyber security was low. While there were some policies available, plans and protocols had not been implemented. The organizations IT department is led by the CISO. However, it was not specifically clear for everyone what the CISO's role was. Due to the size and low cyber security maturity of the organization, there had not been any alignment with other stakeholders who could, for example, assist in the case anything went wrong, or to share knowledge and best practices with regarding cyber threats. Due to the fact that the major and our contact person had a personal connection, it was luck that this person could assist on the spot and had a professional background in similar events.
Post Factors	The communication strategy that was chosen was based on transparency and. The municipality decided that it wanted to act as an example from other organizations and that they could learn from this. During the event, a decision had to be made for who was going the be in control. The municipality or another governmental branch. By staying in the lead, the municipality prevented that a team was making the decisions that was not aware of the internal organization within the systems of the municipality of Lochem.

Table 13: Municipality of Lochem Interview

Date: 3rd of December 2020 (13:00 – 14:00)

Source: Author