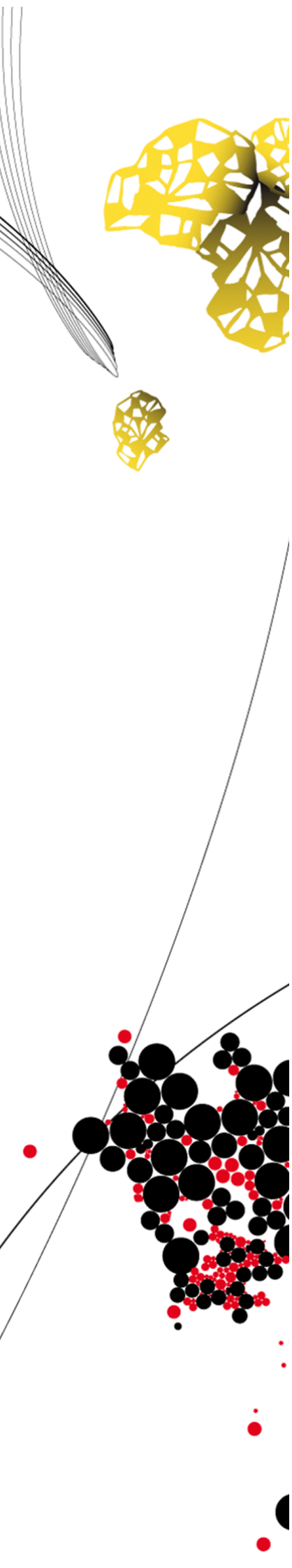


UNIVERSITY OF TWENTE.

Faculty of Electrical Engineering, Mathematics & Computer Science

On the Escalation from Cyber Incidents to Cyber Crises

Riccardo Colombo

M.Sc. Thesis
August 2020

Supervisors:
dr. L. Ferreira Pires
dr. Abhishta

Services and Cyber Security Group
Faculty of Electrical Engineering,
Mathematics and Computer Science
University of Twente
P.O. Box 217
7500 AE Enschede
The Netherlands

Acknowledgements

To dr. Ferreira Pires and dr. Abhishta that have supported me in this journey with extraordinary cordiality and professionalism.

To mr. Renckens that has helped me navigate the challenges of this project with contagious passion for the subject.

To dr. van der Ham for his precious insights and valuable feedback.

To the CERT members for participating in the study with genuine enthusiasm.

To Goewan, Inge, Luuk and all the brilliant people within Northwave that made me feel part of a family since day one.

To Laura and Dario, my mom and dad, that have *always* supported my choices and showed me nothing but love and affection.

To my sister Diana and my brother Alessandro for their continuous support and for always being able to cheer me up with their terrible sense of humor.

To my lifelong friend Stefano for his invaluable advice and for always being present.

To my best friends Alessandro, Luca and Federico for constantly pushing me to go the extra mile.

To my friend Priyanka who supported me in a tough moment with her breezy attitude.

To frozen pizza for comforting and powering me when no one else could.

Without each and every one of you this achievement would have never been possible. Thank you!

Abstract

Cyber crises have increasingly become a reality that severely threatens the survival of contemporary businesses. Recognising when a cyber incident has the potential to become a cyber crisis constitutes an extremely sensitive and fundamental step as it embodies the shift from a tactical to a strategic level of response. Nonetheless, academic research on the transition between the two has been identified to be lacking despite of its importance. The main objective of the present research is therefore that of investigating what factors become of influence when considering the transition between cyber incident management and cyber crisis management in a corporate environment. To investigate the topic of analysis we first conducted four semi-structured interviews with members of Northwave's Computer Emergency Response Team (CERT). The aim was to leverage their experience as incident responders to investigate how companies deal with managing the cyber incidents/crises in the context of their engagements. We then analysed the cyber crisis that Maastricht University underwent in December, 2019, to investigate whether it arose suddenly or if it manifested as the last stage of a sequence of cyber incidents. Lastly, we conducted a semi-structured interview with a Northwave senior incident response coordinator to examine a cyber crisis as well as to explore what challenges become prominent while managing a cyber crisis. We concluded that although cyber crises appear to arise suddenly to client organisations, they instead materialise as the last manifestation of a sequence of cyber incidents. The vast majority of the client organisations have in fact been identified not to have a security monitoring solution in place. This prevents them from observing the transition that leads cyber incidents to escalate to cyber crises and, consequently, from treating them in order to avert the crisis.

Contents

List of acronyms

CERT	Computer Emergency Response Team
ISO	International Organization for Standardization
NIST	National Institute for Standards and Technology
ISIRT	Information Security Incident Response Team
PoC	Point of Contact
CSIRT	Computer Security Incident Response Team
CMP	Crisis Management Plan
CMT	Crisis Management Team
CMDB	Configuration Management Database

Chapter 1

Introduction

When written in Chinese, the word 'crisis' is composed of two characters. One represents danger and the other represents opportunity.

John F. Kennedy, 35^{th} U.S. president

1.1 Motivation

Over the last two decades, digitalisation has significantly revolutionised the way companies run their business, effectively initiating the transition to the information age. What was once recorded on paper and then clustered in physical archives is now being stored digitally in internal databases and in the cloud, giving employees all around the world an easy and immediate way to access the company's assets. At the same time, full scale adoption of computers and automation – coupled with the ever increasing ubiquity of the Internet – has led Industry 3.0 to full maturity and paved the way for the development of Industry 4.0. The combination of both transformations inherently compelled a wealth of modern companies to have a strong digital presence, fostering the integration and development of digital services while inevitably exposing them to the threats of the cyberspace.

Depending on the skills, motive and resources of cybercriminals, businesses can be exposed to more or less sophisticated attacks, which in turn result in a vast range of consequences. More rudimentary attacks may, for instance, compromise few machines with the intention of exploiting their computational power to mine cryptocurrencies, while more advanced attacks may exfiltrate a high volume of confidential data for extortion or lure employees into making unauthorised financial transfers to malicious actors. When a cyber incident has the potential to not only hinder daily operations but to also threaten the organisation as a whole, putting its reputation and stakeholder engagement at stake, it can quickly evolve into a cyber crisis that threatens a long lasting impact on the entire organisation.

The cyber crisis that Maersk underwent in 2017 is a clear example of how a cyber incident can quickly get out of control and spiral into a company wide crisis. On June 27^{th}, 2017, one of the machines running in the Ukrainian branch of the Danish business conglomerate got infected by NotPetya – a piece of ransomware that was engineered to proliferate rapidly from the infected system to all the others that it could get access to. Quickly, the malware spread from that one machine across the whole Maersk infrastructure, not only in Europe but all around the world. The result was complete disruption of operations, affecting 1,500 applications for 49,000 users over 500 locations and causing a company wide crisis [1]. Beyond the direct financial losses that have been estimated to amount to $300 million [2], the crisis had an impact on the company's image and reputation, which if not well managed could have had a catastrophic impact on customer churn rate and shareholder value [3].

Examples of cyber crises like the one mentioned above are a reality that highly worries corporate executives when considering the near future, as highlighted in the 2019 global survey on crisis preparedness published by PwC that involved more than 2.000 executives ($n = 2084$) across 25 industries and operating in 43 different countries [4]. The survey revealed that seven out of ten executives had experienced at least one crisis over the previous five years, while the percentage that had experienced at least two crises amounts to 44%. The most popular crisis triggers are both financial/liquidity (23%) and technological failure (23%), while cybercrime (16%) notably ranks in the top five. Of particular relevance are the results that express the concern for future crises, where cybercrime ranks at first place (38%), closely followed by competitive/market disruption (37%).

1.2 Problem Statement

In this context, understanding when a cyber incident has the potential to become a cyber crisis, and consequently activating the crisis response process in a timely manner, constitutes an extremely sensitive and fundamental step. The transition from incident to crisis, in fact, embodies the shift from a tactical to a strategic level of response, allowing the organisation for a more holistic and proactive handling of the situation.

Nonetheless, while a rather vast body of research is present on the topics of corporate crisis management and cyber incident management, academic research on the transition between the two seems to be lacking despite of its importance. The scarcity of empirical studies in the field of information security had already been identified in [5], where it is highlighted how the inherently sensitive nature of information security leads most companies to turn down research proposals, and to only cooperate with researchers when a high level of mutual trust is present. Moreover,

the lack of literature that explicitly considers the escalation from cyber incidents to cyber crises has been identified in a preliminary phase of the current research. Furthermore, cyber crisis management represents a relatively novel research stream and consequently little academic literature is available on the topic, as it has been highlighted in [6] and further discussed in Chapter 2.

The contribution of the present research is therefore twofold: on the one hand it provides and empirical exploration of a topic that has not received significant academic attention and for which available resources are minimal; on the other hand it gives companies an indication of which factors become of relevance when transitioning to a cyber crisis, consequently acting as a starting point on which to further develop their overall cyber resilience.

1.3 Research Question

The present research investigates how cyber incident management and cyber crisis management are dealt with in a corporate environment, focusing explicitly on how the two are linked and on how the transition between the two is handled. The core of the research concentrated on identifying influential factors that come into play when cyber incidents evolve into cyber crises, considering academic literature and featuring interviews with stakeholders. The main research question, and two related sub-questions, have been formalised as follows:

1. What are the factors that influence the transition from cyber incident management to cyber crisis management?
    (a) At what point does a cyber incident escalate into a cyber crisis? What are the differences between cyber crises and regular crises in this context?
    (b) When transitioning to a cyber crisis, which aspects require cooperation between the incident response team and the crisis management team?

1.4 Method

The research project has been conducted in the scope of an internship as part of the Behaviour and Training unit within Northwave [7], one of the Dutch leading companies in the field of cybersecurity and based in Utrecht, the Netherlands. We have opted to follow a qualitative research style as it allowed us to better approach the complexity of the environment while giving an insight on the different views and perspectives of the challenges that the research sets to tackle. Qualitative research

was also preferable in this case due to the inherently confidential nature of the topic, which makes publicly available literature rather scarce [5].

The first step of the project consisted of performing a literature review that provided the structured background necessary to approach the investigation of the research questions. As literature that explicitly analyses the transition from cyber incidents to cyber crises has been identified to be lacking, the review considered how cyber incident management and cyber crisis management are dealt with in a corporate environment, as well as how cyber crises pose unique challenges to corporate management and leadership. The literature review consequently provided the necessary context to more precisely frame the research question and approach its investigation.

To conclude that academic literature on the transition from cyber incident management to cyber crisis management is lacking we followed a structured approach. First, we conducted a Scopus [8] search that considered the keywords *incident management* and *crisis management* in combination with: *cyber*, *information security*, *escalation*, *transition* and *invocation*. The obtained results were then ordered by relevance and a first assessment to determine their significance was performed by considering their title. Second, for the articles that were identified as potentially significant, we conducted a deeper assessment by reviewing their abstract, introduction and conclusions. Lastly, the articles that were deemed significant were read in their entirety. Additionally, to extend the reach of the analysis we performed a backward search – by reviewing the citations of the articles identified in the previous step – as well as a forward search – by reviewing the articles citing the ones previously identified – as suggested in [9].

Furthermore, the same approach was taken to identify the relevant literature that is presented in Chapter 2. In particular, to define the Scopus search that aimed to identify resources regarding incident management in the context of cybersecurity we took inspiration from [10] and performed the following query: (“incident management” OR “incident response” OR “computer emergency response” OR “security incident”) AND (“cyber” OR “information security” OR “computer security” OR “ict”); while resources regarding corporate crisis management were identified with the following: (“crisis management” OR “crisis response”) AND (“corporate” OR “organisation” OR “cyber”). In addition, the same steps of backward and forward search were performed to extend the reach of the review.

Once the theoretical base was set, an exploratory approach was undertaken in the following steps:

1. Conducting semi-structured interviews with members of Northwave’s CERT. The team gets often engaged as an external resource by companies that fall victim of extensive cyber attacks and for which they do not possess the people,

the resources or the capacity necessary to autonomously resolve. Our aim was to leverage first hand experience to investigate how companies deal with the management of cyber incidents/crises in the context of such engagements.

2. Considering and analysing the case of the ransomware attack that hit Maastricht University in December 2019. The previous step has highlighted the absence of a formal transition from cyber incident management to cyber crisis management in the context of the CERT engagements and we identified the lack of security monitoring as one of the main drivers. Therefore, the objective of this step was to explore a real case to support the above mentioned consideration while suggesting how security monitoring could have averted the cyber crisis by detecting the incidents that led to it, therefore allowing for corrective action.

3. Conducting a semi-structured interview with a senior incident response coordinator of Northwave's CERT. The objective was to validate the findings obtained in the previous steps as well as to investigate which tasks and which challenges are most prominent when managing cyber crises. This has been done by examining a concrete case while also engaging in more comprehensive considerations on the basis of the interviewee's extensive experience regarding cyber crises.

1.5 Thesis Structure

The remainder of the thesis is organized as follows: Chapter 2 introduces the background necessary to structure the theoretical framework as well as to put the research into context; Chapter 3 describes how the interviews with members of the CERT have been structured, it presents the main findings and discusses them; Chapter 4 presents and discusses the cyber crisis that Maastricht University underwent in December 2019 considering the sequence of events that lead to it; Chapter 5 presents the discussion on a ransomware attack for which the CERT has been engaged, considering what challenges emerged during the management of the crisis while also engaging in more comprehensive considerations based on the experience with analogous cases. Finally, Chapter 6 draws the conclusions of the research and discusses its limitations.

Chapter 2

Background

As highlighted in Section 1.1, cyber crises can result in really severe consequences for a business and are a reality that profoundly worries company executives, especially when looking into the future. This is confirmed and further reinforced by the 2020 edition of the annual risk barometer published by Allianz [11]. For the first time ever the survey ranks *Cyber Incidents* as the most significant business risk for companies with 39% of the responses, overcoming the long lasting top peril *Business Interruption* (37% of responses) and leading the third most popular risk *Changes in Legislation* (27% of responses) by a distance. Considering that seven years ago cyber incidents ranked 15^{th} with only 6% of the responses, this result highlights even more the relentless pace with which the threat landscape in the cyberspace evolves, driven by businesses increasing their reliance on the digital infrastructure as well as by a number of high-profile incidents taking place.

Although the majority of the most notorious cyber incidents - such as Stuxnet [12], Shamoon [13] and more recently NotPetya [2] - appears to be state sponsored and to target some of the biggest organisations in our society, the threats of the cyber space are not something that only big corporations should worry about. The dark market for malware is in fact increasingly getting traction and becoming financially accessible to the most; banking trojans and ransomware kits can be found cataphract in easy to use applications that can cost as little as a few hundred dollars [14], [15]. This significantly lowers the barriers to the entry, allowing average skilled criminals to mount relatively sophisticated attacks on vulnerable businesses without having to develop the malware themselves. As a result, over the last decade the cyber insurance market saw a rapid increase in the number of subscriptions. A report published by Zurich in 2018 shows in fact that while only 35% of the surveyed corporations had a cyber insurance subscription in 2011, the percentage steadily increased over the following years leading the market penetration to reach 75% in 2018 [16]. However, while having a cyber insurance can undoubtedly lower the direct cost of a successful cyber attack, the potential impact of cyber crises go far

Figure 2.1: NIST Cybersecurity Framework [18].

beyond the direct financial damage of the cyber attack, posing a direct threat to the company's reputation, stakeholder engagement, customer churn and devaluation of stakeholder value as discussed in [17] and in [3].

Therefore, developing cyber resilience is an effort of paramount importance in the current business environment. Responding effectively to a cyber crisis is without any doubt a critical capability that can make the difference between the survival and the extinction of an organisation. However, it is worthwhile to highlight that crisis response in isolation is not sufficient to grant an adequate level of resiliency, but it rather has to be considered in combination with a set of complementary capabilities. Before deep-diving into cyber crisis management it is therefore beneficial to briefly introduce the National Institute for Standards and Technology (NIST) cybersecurity framework [18] with the objective of framing the response capability within the overall strategy.

The framework provides organisations with guidance on how to assess and develop their security posture by identifying numerous tiered activities that can be organised into the 5 core functions portrayed in Figure 2.1. Firstly, the activities featured in the *Identify* function aim at giving a holistic perspective on the business context, gaining awareness on which resources support the critical business processes and analysing the related cyber risk. This provides a baseline on which organisations can prioritise their efforts while staying in alignment with their risk management strategy and business needs. Based on the previous step, the *Protect* function leads organisations to envision, design and implement security controls that mitigate the identified risks. The security measures will act as preventive measures against malicious activity whose top priority is to secure the business critical processes. Once

the safeguards are in place, the organisation can implement the activities necessary to timely identify the occurrence of a cybersecurity event. This ensures that threats emerging from the residual risk arisen from the previous step will be timely identified, giving the organisation the opportunity to engage in the reactive activities outlined in the *response* function and that deal with the containment of the impact of a potential cybersecurity incident. Lastly, the recover phase focuses on maintaining plans to restore services and capabilities that are affected by the cyber incident, highlighting the importance of timely restoring normal operations to mitigate the extent of the impact.

2.1 Cyber Incident Management

To align on a shared terminology – while better framing how incident management is defined in the context of information security – the following list introduces three relevant definitions that are featured by the International Organization for Standardization (ISO) in ISO/IEC 27000:2018:

- *Information security event*: "identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that can be security relevant" [19, p.4].
- *Information security incident*: "single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security" [19, p.4].
- *Information security incident management*: "set of processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents" [19, p.5].

Incident management is therefore defined as a set of processes designed to effectively deal with security incidents, and several frameworks are available to provide guidance on their implementation. To understand which of those frameworks are actually used in practice, Tondel et al. [10] conducted a systematic literature review that explored current practice and experiences on incident management in a variety of organisations. The research highlighted that although various frameworks are available, only two of them stand out when considering common practice: ISO/IEC 27035:2011 "*Information Security Incident Management*" [20] and NIST Special Publication 800-61 rev. 2 "*Computer Security Incident Handling Guide*" [21]. Moreover, after conducting a comparison between what ISO/IEC 27035:2011 prescribes and the experience reported by the considered case studies, the authors

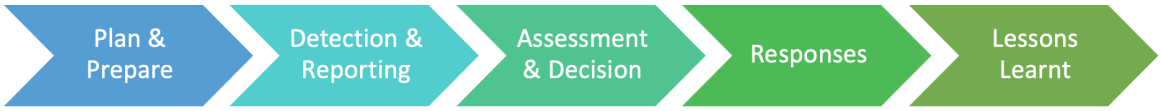


Figure 2.2: Phases of ISO/IEC 27035:2011 [20].

were able to conclude that, despite the identification of several challenges, current practice seems to generally be in line with the standard.

2.1.1 Incident Management Process

Although ISO/IEC 27035 and NIST SP800-61r2 share many similarities, both in structure and content, and both constitute a valid approach towards incident management, the former benefits from being developed by an international organisation driven by experts worldwide. Therefore, this section will use ISO/IEC 27035 as a reference to outline the main activities that are prescribed for the different phases illustrated in Figure 2.2:

1. *Plan and Prepare:* the objective of this phase is to define a number of preparatory activities that will provide the necessary foundation to effectively tackle the operational challenges that will arise in the subsequent phases. Relevant activities that should be performed in this phase include: formulating an incident management policy and integrate it in other existing policies (e.g., information security policy); define an incident management scheme that encompasses forms, procedures and tools necessary to handle security incidents (e.g., incident classification scale); establish an Information Security Incident Response Team (ISIRT); establish relationships with organisations involved in the incident management process; and test and assess the incident management scheme.

   Depending on the size and structure of the organisation, management may decide to adopt a dedicated team, a virtual team, or a mix of the two. Moreover, as responding to a cyber incident may lead the organisation to involve external resources - such as an external Computer Security Incident Response Team (CSIRT) - it may be relevant to take contacts with those organisations at this stage [21].

2. *Detection and Reporting:* once the necessary preparations are put in place, the framework focuses on the operational part of the process. This phase deals with the detection and reporting of any occurrence of a security event, highlighting that such events can be detected in multiple ways, both manual

and automated. Relevant information related to the security event must be collected and stored; moreover, it must be ensured that electronic evidence is gathered and securely protected. Lastly, all activities must be logged and the security events registered and tracked in an incident tracking system.

In this regard, NIST SP800-61r2 specifies how the signs of an incident that can lead to detection fall in two categories: *precursors*, which act as a warning that an incident may occur in the near future; and *indicators*, which instead manifest either during or after the incident and therefore identify its occurrence. Moreover, the framework highlights how most attacks do not possess any identifiable precursor, consequently expressing how timely and accurately detecting a cyber incident is among the biggest challenges that organisations face throughout the whole incident response process [21]. This holds true especially when considering data breaches, a recent study published by IBM reported in fact how the mean time to detect a data breach caused by a malicious cyber attack amounts to 230 days [22].

3. *Assessment and Decision:* once the security event has been detected and reported, the designated Point of Contact (PoC) should first assess it and then determine whether the event should be classified as a security incident or not. In case the PoC classifies the event as a security incident, the ISIRT should perform a second assessment to confirm the initial evaluation of the PoC; the assessment should be conducted considering the classification scale defined during the Plan and Prepare phase. Once the event is assessed and reported, responsibilities for handling the incident should be assigned and formal procedures should be provided for the notified persons to follow. Every step and every decision should be logged for both clarity and accountability.

   Assessing the extent and magnitude of the impact of an incident is an activity of fundamental importance as it inherently determines how the incident will be handled. Nonetheless, this activity is reported by [21] as the most challenging part of the whole incident response process for many organisations, consistently with what has been discussed in [23] and [24].

4. *Responses:* this phase focuses on the response actions taken on the security incidents and performed in accordance with what has been assessed and decided in the previous phase. Internal resources necessary to handle the security incident must be assigned and potentially needed external resources identified. Security forensics analysis should be initiated accordingly to the scale of the security incident. The ISIRT is entrusted to perform the agreed responsive action and to continuously review whether the incident is under control or not. In the latter case, the ISIRT should further escalate the incident

and start the procedure of crisis invocation. The occurrence of the security incident as well as any other relevant detail must be communicated to designated internal and external people or organisations, especially to those involved into the management and resolution of the security incident. If deemed necessary, an external CSIRT may be activated to mitigate the incident during this phase.

5. *Lessons Learnt:* this phase takes place once the security incident has been resolved/closed and it involves reflections and learnings on the incident. The key activity of this phase consists in reviewing, identifying and making improvements to the information security incident management process, reflecting on what has not been sufficiently effective and considering what has instead worked satisfactorily. Moreover, further forensics analysis should be performed when required and the results of the incident review could be shared - if the organisation wishes to do so - with a community of trusted professionals and peer organisations.

2.2 Crisis Management

Crisis management is an extremely vast and multidisciplinary research domain that analyses how crises are dealt with under different perspectives. Despite the heterogeneous spectrum of current research, of which a taxonomy is given in [6], the core elements that characterise a crisis are shared among the different research streams and reflected in their definitions of crisis:

> "*A low-probability, high-impact event that threatens the viability of the organization and is characterized by ambiguity of cause, effect, and means of resolution, as well as by a belief that decisions must be made swiftly.*" [25, p. 60]

> "*A serious threat to the basic structures or the fundamental values and norms of a system, which under time pressure and highly uncertain circumstances necessitates making vital decisions.*" [26, p. 2]

> "*An unprecedented or extraordinary event or situation that threatens an organization and requires a strategic, adaptive, and timely response in order to preserve its viability and integrity.*" [27, p. 6]

Analysing the aforementioned definitions it is possible to note how, although different in details, they share four main elements that characterise crises and set them apart from incidents. In particular, while incidents are to some extent foreseeable and cause minimal to minor impact, crises are *rare events* that threaten organisations on a *strategic level*. Moreover, crises develop in a context of *high uncertainty*

Table 2.1: Differences between incidents and crises [27].

Characteristic	Incident	Crisis
Predicatbility	Generally foreseeable although unpredictable in detail. Can be addressed with pre-planned measures.	Complex, unique and uncertain. It poses exceptional challenges.
Onset	No-notice or short notice disruptive events. It can emerge through a gradual failure or loss of control.	Sudden or no-notice, it can emerge from an incident that has not been contained or has escalated with immediate strategic implications.
Urgency and Pressure	Limited sense of urgency, response has a short resolution time.	High sense of urgency, response has longer resolution time.
Impact	Manageable impact although potentially widespread. It does not lead to unmanageable collateral damage.	Strategic impact that threatens the entire organisation. It can transcend organizational, geographical and sectoral boundaries.
Media Scrutiny	Little to no media attention.	Significant media attention that threatens reputation.
Manageability	Can be mitigated with predefined procedures and plans.	Requires a flexible and adaptive response.

and ambiguity where decisions have to be taken under *time pressure*. By contrast, incidents are reasonably well understood and get resolved over a short time frame. To extend the comparison, Table 2.1 gives an overview of the analysis of the factors that differentiate crises from incidents that is given in [27].

2.3 Cyber Crisis Management

The field of cyber crisis management is still relatively novel when compared to more traditional crisis management research streams and it has not yet gained much traction in the academic world. Kuipers et al. [6] conducted a taxonomy study of academic articles published by three independent journals specialised on the topics of crisis and disaster management over the previous 34 years. The research showed

how only 6% of the articles[1] focuses on ICT/Cyber crises. Although small, the number may seem significant at a first glance; however it must be considered that for how the category has been designed, a wide variety of IT-related topics are included (e.g., communication technologies and sociotechnical disasters) and cyber crises therefore only represent a slight portion of the initial percentage.

The shortage of academic research on the topic is also a contributing factor on the lack of shared agreement on a general definition of cyber crisis, highlighted in [28] where the author encountered a substantial absence of agreement on the definition of cyber crisis when examining different European approaches to national cyber crisis management. Nonetheless, providing a definition is important to align the reader with the author on the meaning of cyber crisis. The Israeli Government recently published a report that discusses national cyber crisis preparedness and management; in the document a cyber crisis is defined as:

> *"A situation posing a real threat of damage, or actual damage, to a vital cyber asset, which is liable to cause critical damage to routine operations, reputational damage, economic damage and endanger human lives."* [29, p. 6]

The definition is able to depict the nature of a cyber crisis while highlighting its disruptive potential, although it may be regarded to overly focus on the impact of the crisis while neglecting other distinctive features. The reader should therefore recall what has been previously discussed and enrich the context of the definition with the notions of urgency, uncertainty and singularity that are distinctive of crises.

2.3.1 Distinctive Factors

Although similar to regular crises for some aspects, cyber crises are characterised by a number of distinctive factors that are peculiar of cyber incidents and that expose cyber crisis managers to unique challenges - an overview is given in Table 2.2.

Firstly, incidents that manifest in the cyberspace inherently transcend the limits of the physical world, both in terms of propagation speed and in terms of physical boundaries. Opposed to traditional incidents, cyber attacks have in fact the unique advantage of being able to travel at the speed of the Internet, allowing for the potential of covering enormous distances in few instants while transcending geopolitical borders. Exemplary of these characteristics is the NotPetya campaign; after having gained access to a single system in the victim's infrastructure, the malware was able to quickly spread to all the other departments of the branch to then propagate - in a timespan inferior to ten minutes - to the whole infrastructure across the

[1] Computed as the average of the percentage for each journal.

Table 2.2: Distinctive factors of cyber crises.

Characteristic	Description
Propagation	Unlike the vast majority of other incidents, cyber incidents have the potential of propagating very swiftly across the organisation and of turning into a crisis in a matter of minutes.
Transboundary	The cyberspace inherently transcends geographical and political borders, incidents can quickly travel across boundaries and sectors to suddenly magnify their impact.
Tight Coupling	Modern systems are highly interconnected and often dependent on each other, a cyber incident affecting one system can leverage connectivity to move laterally and affect all the connected systems.
Singularity	Incidents that exploit zero day vulnerabilities can be extraordinarily disruptive as their novelty allows them to evade safeguards and affect a vast amount of devices.
Attribution	Anonymity is more easily preserved in the cyberspace than in the physical world, which renders attribution particularly troublesome.

globe [2]. Moreover, the digital transformation has lead corporate infrastructures to increasingly become hyperconnected and reliant on each other, both within the organisation itself and with external partners. In particular, complex chain dependencies can quickly increase the complexity of timely identifying and addressing the root cause of an issue; while this may also be true for some traditional scenarios, the increasingly popular trend of adopting outsourced cloud solutions, coupled with the high demand for software as a service have significantly increased tight coupling and cyber dependency [14].

Furthermore, zero days exploits can add an unprecedented degree of novelty to cyber attacks. This kind of exploits leverage software vulnerabilities that are not know to both the software users and the software vendors. As a consequence, no software patches are available, allowing for the potential to affect a significant amount of systems with no practical way to prevent it. Exemplary is the case of Stuxnet where the malware leveraged four different zero day exploits to covertly sabotage operational machinery in an Iranian nuclear facility [12]. Lastly, cyber criminals are able to leverage the ubiquity of the internet not only to cross political borders but also to operate with a high degree of anonimity, which inherently leads the activity of attribution to being particularly complex.

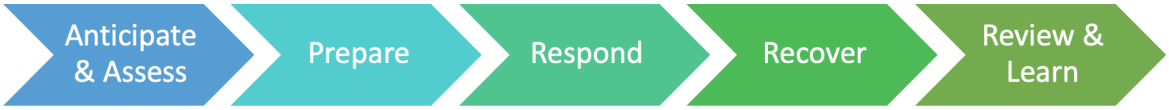


Figure 2.3: Phases of CEN/TS 17091:2018 [27].

2.4 Crisis Management Process

"*Crisis management – Guidance for developing a strategic capability*" [27] implements a European technical specification - CEN/TS 17091:2018 - that provides organisations with a set of principles and good practice guidance to foster resilience by implementing effective crisis management capabilities. In the specification, crisis management is formally defined as "*the development and application of the process, systems, and organizational capability to deal with crises*" [27, p. 7]. While the document discusses several topics that need to be considered when dealing with crises, this section focuses on outlining the main components of the five-phases framework to develop crisis management capabilities presented in [27].

As a first activity, the top management should establish, define and document a *crisis management policy* that will serve as the basis on which to further develop the planning and implementation of crisis management procedures. The policy should include a clear and concise definition of the management's objectives when handling a crisis, a broad overview on how the management intends to reach those objectives, as well as their commitment to high standards. Furthermore, the policy should identify the people responsible for its different components, establish priorities and appropriate resources, and define the roles and responsibilities necessary to implement all crisis management capabilities.

After having described what a crisis management policy should include, the technical specification discusses each of the five phases that constitute the framework and depicted in Figure 2.3. The following list represents a digest of those phases which is meant to spotlight the most salient activities featured in the different phases:

1. The main focus of the *anticipate and assess* phase is to set up a system able to intercept early warning signs of potential crises as well as to structure a horizon scanning process able to identify potential crises in the medium to long term. At this stage the organisation should have a clear understanding on the relationship between different internal components - such as risk management and business continuity management - and it should recognise that crises can arise regardless of the effectiveness of the security controls that are put in place.

2. The *prepare* phase is by far the most extensive and it revolves around three

main components: the crisis management plan; information management and situational awareness; and the crisis management team (CMT). The main goal of the *crisis management plan* (CMP) is to provide a concise guideline able to support the CMT when dealing with a crisis; as planning for every possible crisis is not only unpractical but also unrealistic, the plan should be generic and not scenario specific. The CMP has to clearly state who holds the authority necessary to take key decisions, it has to define roles and responsibilities and it has to provide information on crisis communication and key contact details. The CMP should also describe the crisis activation mechanism, define both the structure and the role of the CMT and provide tools and templates that can support the crisis management plan. *Information management* focuses on diminishing the level of uncertainty by gathering, evaluating, filtering and making sense of new information that will then have to be appropriately presented to the decision makers. *Situational awareness* deals instead with gaining an understanding on what is happening, on the degree of uncertainty and on the degree of containment while attempting to identify what is most likely to happen in the near future. Lastly, the composition of the *crisis management team* should be defined. Although the framework presents a list of possible roles that can be included in the CMT, its composition and structure highly depends on the size and structure of the organisation as well as on the nature of the crisis.

3. While specific actions are impossible to plan due to the unpredictable nature of crises, the *response* phase presents examples of generic activities that can be performed by the CMT while managing the crisis. Important tasks of this phase include achieving and continuously reviewing situational awareness, defining the strategic direction of the response and ensuring that concise yet effective meetings are regularly performed. Furthermore, monitoring both internal and external communication and monitoring the response to ensure that priorities are understood and that the response is in harmony with the strategy represent activities of fundamental importance.

4. The main objective of the *recover* phase is to deal with the effects and the impacts that the crisis has caused in order to return to a new normal. The recovery effort needs to be supported by appropriate funding and it often has to address long lasting consequences (e.g., reputational damage or ongoing legal and insurance challenges). Additionally, the framework highlights how this phase can be seen as a chance of leveraging opportunities that may have stemmed from the crisis to regenerate, restructure and realign the organisation.

5. *Review and learn* constitutes the terminating phase of the framework. The central idea is to analyse and assess the performance of the organisation during the crisis - whether it was real or simulated - to identify learning lessons and areas to further improve plans and procedures. At this stage it is paramount to not only identify lessons but to also address them; process that is often neglected according to the authors.

2.5 Crisis Leadership

Boin et al. [26] build on ten years of research on crisis management to identify five core tasks that leaders are called to perform in time of crisis. It is worthwhile to present the core tasks as they give an indication on which activities have to be performed, as well as what critical points may arise, while managing a cyber crisis.

The task of *sense making* becomes critical when leaders find themselves on the verge of an imminent crisis. At this stage they are called to work towards an understanding of the situation while operating in an environment of high pressure and high uncertainty. Leaders have to draw from signals that come from several different sources and which are often vague, contradictory, and inaccurate, to assess how threatening the unfolding events are, what kind of consequences they may cause, and foresee how the situation will develop. Trimintzios et al. [30] remark how this phase is not characterised by a lack of information but rather by an overload of it. What lacks is instead the value of such information; meaningful information is in fact often buried under several layers of noise and irrelevancies.

Once a certain degree of understanding of the situation has been reached, leaders have to build a message that frames the crisis and convey it to others. *Meaning making* deals with constructing a coherent picture of what is happening and combining it with credible storytelling that covers what are the causes, what is at stake, and what can be done to deal with the situation. This task is of extreme relevance as the following decisions will build on the vision that has been constructed in this step. Therefore, it is possible to see how when leaders fail at conveying a convincing scenario, their subsequent decisions will most likely be questioned and not respected. Moreover, it must be stressed that leaders are not the only ones attempting to frame the crisis: news outlets, reporters and social media play an active role in rushing to some interpretation of the situation. Good leaders must retain a level of control over the public image of the crisis and ensure that the organisation's official channels act as the main source of public information.

Decision making represents a challenging task as leaders are often confronted with issues that they are not familiar with and that fall outside of their expertise. Nonetheless, leaders are called to take strategic decisions on the base of incom-

plete and unreliable information with limited time to reflect and consult with others. As the situation remains unclear and volatile, leaders may become overly invested in operational challenges and may end up micro-managing field work instead of delegating tasks and keeping their focus on the long-term strategy [30].

Once the crisis has been managed and the situation de-escalates, *terminating* becomes a key task. Leaders are now called to initiate the transition from crisis to routine, easing the organisation in what can be defined as the new normal. It is important to note how transitioning to this stage does not necessarily entail that every aspect of the crisis is resolved, it rather means that what is still left unaddressed can be resolved with routine procedures. As a crisis is an unprecedented event that tests the organisation's resilience on a strategic level, ensuring that such rare and singular experience is processed into *learning* is a crucial task. Despite the opportunity of offering the organisation a fresh look and genuine improvements, the authors identify learning as a highly underdeveloped task. This is mainly due to the fact that in order to accept change, management has to admit its failures and to some extent question its previous position; alternatively, opposing forces may address improvements as failures of the management that will in turn reject learnings not to be at fault. Leaders are then left with the arduous challenge of navigating through blame games and political strategies to align interests and foster organisational learning.

2.6 The Opportunity of Effective Crisis Management

The previous sections have highlighted how crises can threaten organisations' survival and have given an overview on how management of such disruptive events can be approached. This section focuses instead on showing how crises can be also seen as opportunities; effective management can in fact showcase resilience to shareholders that will in turn positively re-evaluate the profitability of the organisation triggering an increase in shareholder value.

To determine to what extent effective management can represent an opportunity for growth, Pretty [3] conducted a study that analysed the impact of 125 corporate crises on shareholder value. The research identified two very distinct groups from the original firm portfolio: *winners* and *losers*. The two groups differentiate themselves in the way the market reacts to the crisis in the following trading year: winners were able to gain an average of 20% on shareholder value while losers experienced an average loss on shareholder value of almost 30%.

To support the findings the author highlights how in time of crisis the market receives an amount of information on both the company and its management that is much more significant when compared to the information received in regular circumstances. Shareholders use the additional information to re-assess their expectations

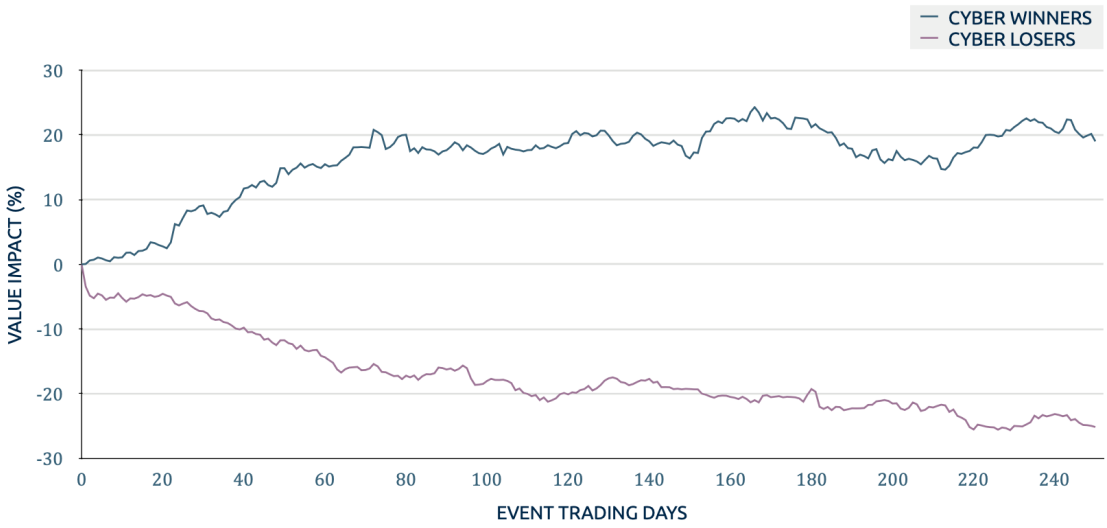


Figure 2.4: Cyber winners and cyber losers [3].

on the future performance of the company and the assessment is then reflected on the stock price. When management impresses, expectations for the future exceed the pre-crisis evaluation. When management instead disappoints, investor's confidence on the future growth of the company decreases and shares value diminished as a consequence.

To conclude, the author has also analysed the impact that crises arising from cyberattacks have on shareholder value in isolation. The analysis on the sub portfolio - that accounts for 23 out of the 125 crises of the original portfolio - obtained consistent results which are displayed in Figure 2.4. In particular, cyber winners gained an average of 20% while cyber losers lost an average of 25% on shareholder value. This result is significant as it highlights how cyber crises can cause consequences comparable to the ones arising from regular crises, reinforcing the notion that the effects of cyber crisis are not limited to the digital world but can rather result in serious strategic implications. Consequently, this result is in accordance to what has been discussed in [4] and [11].

Chapter 3

Interviews with Northwave's CERT

Chapter 1 has identified a lack of literature that considers the transition from cyber incidents to cyber crises, as well as cyber crisis management more broadly. Information security represents a sensitive subject for organisations, leading them to be reluctant to share delicate data for research purposes. To overcome this challenge, we decided to adopt an exploratory approach by conducting semi-structured interviews with four of the members of Northwave's CERT. The role of a CERT can be intuitively described drawing an analogy with a fire department [31]. In fact, the same way the fire department has an emergency number that can be dialed to request for help in case of a fire outbreak, the CERT has an emergency number that can be dialed to request for help in case of a security incident. Similarly, as the fire department can respond by deploying a team of firefighters, the CERT can respond by deploying a team of incident responders. The team gets therefore often contacted by companies that fall victim of extensive cyber attacks for which they do not possess the people, the resources or the capacity necessary to autonomously resolve. The CERT is then engaged as an external party with the objective of resolving the cyber incident and restoring the company's operations. Although Northwave's CERT does not directly constitute part of the client organisation, the team is nonetheless actively involved in managing the consequences of the attack and can therefore offer a perspective based on first hand experience on this topic.

3.1 Method

In order to explore the transition from incident to crisis through the experience of the CERT members, we have decided to adopt semi-structured interviews as the principal data collection method. Questionnaires and structured interviews offer the advantage of obtaining results that can be more easily compared with each other, leading to a more quantitative interpretation of the primary data. However, such

methods are best suited for instances where well defined background knowledge is present, and were consequently assessed to lack the flexibility needed in our exploratory approach. Semi-structured interviews allow instead the researcher to be more agile and to adapt the conversation to accommodate unexpected findings and information, while allowing for a deeper investigation of complex issues [32]. With this approach: *"the dialogue can meander around the topics on the agenda – rather than adhering slavishly to verbatim questions as in a standardized survey – and may delve into totally unforeseen issues"* [33, p. 493]. Moreover, semi-structured interviews are particularly suitable when wanting to explore the independent thoughts of different individuals in a group. Conversely to a focus group approach, they allow the interviewees to express themselves in complete freedom. Contrasting the element of peer pressure that might lead them not to be candid about their opinion when not approached in isolation [33].

To conduct the interviews, an interview guide has been drafted following the guidelines outlined in [33]. Additionally, a document outlining the process of activation and deployment of Northwave's CERT was analysed in order to structure some of the questions [34]. To cover the whole process the interview guide has been organised in four sections: *background*, *activation*, *deployment* and *crisis transition*. The *background* section primarily aimed at getting context by exploring what are the most popular kind of attacks for which the CERT gets deployed as well as what is the principal motive that drives the attackers. Moreover, this section was also designed with the intention of establishing a rapport with the interviewees by approaching a more conversational topic in the beginning of the interview [33]. The *activation* section focused instead on exploring the activities and challenges that are encountered during the phase of primary triage, how the team approaches understanding the magnitude of the attack during that phase, and whether or not the CERT is contacted in a timely manner. The section on *deployment* explored what are the main topics of discussion during the first onsite meeting with the client, as well as how that relates with the assessment of the business impact and with the prioritisation of the recovery work. Additionally, the likelihood that the client has an incident response plan and a security monitoring solution in place was also explored. Lastly, the section on *crisis transition* was set to explore the incidence with which the attack for which the team is deployed represents a cyber crisis for the client, how likely is it that the client has a crisis management plan in place, and whether cyber crises arise abruptly or offer early warning signals. For completeness, the full interview schema is available in Appendix A.

Although the order of the sections and the order of the questions within each section were structured to naturally follow the process of activation and deployment, the interviews at times evolved unexpectedly and the topics were consequently re-

ordered on the fly to support the conversation to unfold naturally as advised in [33]. Furthermore, we adopted the agile approach discussed in [35], where the interview guide is considered as a work in progress – subject to changes and adjustments as feedback is gathered through the initial interviews. In particular, the first interview helped to delineate which questions fell out of the scope of the activities performed by the team – and were therefore excluded from the guide – while it allowed for new topics to emerge, which led to the introduction of new, more pertinent questions. Nevertheless, after the first iteration only minor adjustments were performed.

The interviews were expected to last around 45 minutes, therefore a time slot of one hour was budgeted for each interview. Critical questions were identified – and marked in advance – to avoid running out of time before having covered them, specific marking and color coding was used to quickly identify relevant keywords[1], and techniques of active listening and mirroring were employed to empower and stimulate the interviewees to share their experience [33]. Moreover, as suggested in [36], during the interviews and before moving to the next topic the main points of the discussion were at times restated, in order to both actively show interest to the respondent and to ensure that the central argument was correctly understood by the researcher. Lastly, when in need of stimulating the interviewee to further elaborate his answer, great benefit has been found in the use of silent probes [37].

A total of four interviews were performed: the first two were conducted digitally by the means of a videoconferencing application while the last two were conducted in person. To minimise information loss, and with the consent of the interviewees, an audio trace was recorded during the in person interviews, while a video recording was saved for the ones conducted digitally. Recording offers both advantages and disadvantages. On the one hand it allows the researcher to engage more actively in the conversation, and to ponder the best next question instead of having to intensively focus on transcribing the answers; on the other hand responders may instead feel inhibited by the recording device and consequently be less incline to expose their personal opinion [33]. We argue however that given the higher level of trust and familiarity between the researcher and the respondents, who belong to the same organisation, the benefits of recording outweighed the drawbacks.

Lastly, convenience sampling was used as a non probability sampling technique [37] as the respondents were identified within Northwave itself. We claim however convenience sampling to be a reasonable approach in this case given the well recognised challenge of getting primary data in the field of information security [5]. Furthermore, convenience sampling also represents a sensible approach as the aim of the interviews was that to identify an exploratory sample. Intended to be used as a mean to examine a new area rather than to offer a representative image of the entire

[1] This was done in a paper version of the interview guide

population [32].

3.2 Findings

Two pieces of information are relevant to outline the background of the interviews in order to contextualise our findings. Firstly, the most prominent type of cyber attacks for which the CERT gets activated – and which accounts for the majority of the engagements – consists of ransomware cases. This type of attack is particularly threatening for client organisations as it extensively impacts the availability of their most critical resources by encrypting (part of) the supporting digital systems. This in most cases substantially halts daily operations which in turn generates a significant sense of urgency. In absence of a well designed backup strategy, the encryption can only be reverted by obtaining the decryption key from the attacker – who asks for a certain financial amount in return (i.e., the ransom). Therefore, in this kind of cyber attacks the cyber criminal is purely driven by a financial motive, as it has been confirmed by the interviewees. Consequently, the scope of the interviews spontaneously focused on ransomware cases. Secondly, Northwave's partnership with an insurance company represents the predominant channel with which client organisations come into contact with the CERT for this kind of engagements. This entails that the team is not familiar with the infrastructure of the organisation, as well as with its business more broadly, when it starts an assignment.

3.2.1 Activation

Primary triage represents the central activity that is performed when a company contacts the CERT for an engagement. The goal of primary triage is to gain a first understanding of what the incident is, what steps have already been taken and how severely it is affecting the business, in order to decide, together with the client, whether the deployment of the team is necessary.

During this phase, having a meaningful and open conversation with the client has been consistently identified as an element of extreme importance by the interviewees. In fact, as cases significantly vary from one another, no hard parameters can be used to systematically score the gravity of the cyber incident. Furthermore, it was highlighted that in this regard the focus point is not to assess the gravity of the incident per se, but to rather put that into the context of the specific organisation. Some companies, for instance, will not experience particularly severe consequences when being offline for a few days, whereas other companies will instead experience thousands of Euros of damage for each hour of downtime. Therefore, having an open and structured discussion, which not only focuses on understanding

the severity of the incident in isolation, but that also puts that into context by getting a sense on the size and nature of the company, and whether business critical processes are affected, is of utmost importance to understand the degree of disruption that the incident entails. In addition, the discussion is also important as it gives the team an opportunity to estimate the scale and nature of the operations that will have to be performed, consequently getting a sense of how to structure the response team in terms of both people and resources. Lastly, being able to get the most complete overview in the shortest amount of time has been identifies as a challenge repeatedly experienced in this phase.

Part of the interview was also directed to understand whether the CERT gets frequently involved at the most convenient time during the life cycle of the incident, or if clients often do not involve the team in a timely manner. A first consideration that has been made by the interviewees is that being ransomware the most popular reason of engagement, which often critically hinders daily operations, clients fairly quickly feel the urgency to seek for external support. In fact, although the full scope of the attack may not always be clear at this stage, the strategic relevance that the impact entails is instead indisputable. Conversely, there might be cases – with business e-mail compromise for instance – where the team is activated with a considerable delay. This is however frequently due to a delay in the detection of the incident rather than in a delay in responding to it. For such cases it is not uncommon that the client only detects the incident a few weeks later when it is notified, for instance, of not having payed the latest invoice by a supplier.

A further reason for late activation has been identified with the client trying to autonomously resolve the incident for too long without succeeding before taking the decision to involve an external party. In this regard, the relevance of the client's IT team being able to realise what their limitations are beforehand has been highlighted consistently. This is not necessarily a question of skills, but also a matter of experience, capacity and resources. Moreover, having an incident response process in place, with a person responsible for it, has been identified as a factor that contributes to delineate when an external party needs to be involved, and consequently to a timely activation. Nevertheless, it was stressed how only a slight fraction of the clients that engage with the CERT do have an incident response process in place. Lastly, having a cyber insurance policy has been identified as another factor that, to some extent, contributes to a more timely activation. Companies that have a cyber insurance policy tend to call more promptly, whereas companies that do not have one tend to rely on their resources for longer before maturing the decision of involving an external party.

3.2.2 Deployment

If during the previous phase it is decided that deployment is needed, an intake meeting is held once the team arrives on site. The meeting consists in an in-depth continuation of the discussion that was held over the phone during primary triage with the objective of assessing what processes are impacted, where do the most critical applications run, setting clear objectives and priorities, and combining it into a plan with clearly defined action points.

The meeting often includes the client giving a brief presentation on the business itself, what the company does, and how it is structured. This step is important as it gives the context necessary to align the digital component of the incident with the business side of it – while also helping to build a relationship with the client. A key activity performed during the initial stages and that builds on the previous discussion consists of mapping the business processes to the IT infrastructure and vice versa. This is of utmost importance to generate a complete picture of the current situation and to understand how to prioritise the subsequent work in order to enable the client to be productive again in the shortest time possible. Priorities are often set in terms of what business processes should be restored first, which is why being able to understand what portion of the infrastructure supports those process is of paramount importance. In this regard, although having punctual documentation on the infrastructure has been identified as a facilitating factor, it has been stressed how most clients do not possess it. This often results in the time consuming activity of having to reconstruct a representation of the infrastructure together with the IT team of the client.

Significant is also the tone and language that is used. As the meeting is attended by both technical and non-technical people, ensuring that everyone achieves a satisfactory level of understanding of the situation may not be straightforward. The interviewees have highlighted how the IT team of the client can at times be very technical in nature and therefore not always proficient in translating the business processes to the IT processes and vice versa. The CERT has built extensive experience by working on a wealth of different cases and has therefore developed the flexibility necessary to support the conversation in a way that both parties can understand. As described by one interviewee: "*we sometimes need to be the party in between, that translates the business story to the IT story and vice versa*". Moreover, this also highlights the importance of getting a sense of the business of the client and its most critical processes.

Lastly, a part of the interview was also directed to investigate how frequently clients have security monitoring as well as a formally defined incident response plan in place. The interviews highlighted that security monitoring is hardly in place, and although sometimes clients do have a monitoring server, it is often the case that

no one is responsible to consistently guard it. Nevertheless, the interviewees emphasized how in most cases a security monitoring process would have detected the attack at an early stage, giving the client time to react to it and avert the crisis.

This is also the case of incident response plans, which in the experience of the team are very rarely in place. Giving a structured approach towards the resolution of the incident has been identified as one of the activities that the client benefits the most from. Part of the value that the team provides has been identified not merely with their technical expertise but also with the experience they developed in solving incidents, which allows them to leverage their skills to structure a plan that will lead the organisation to recovery.

3.2.3 Transition to Crisis

A segment of the interview aimed at examining how the team members characterise the difference between a cyber incident and a cyber crisis. According to the interviewees, incidents can be solved fairly quickly, by following routine plans and procedures, and do not affect the business in a significant way. The scale of the impact and its direct implications on the ability to perform the core business activities has been consistently identified as the main driver that dictates the difference between the two, although the interviewees agreed that quantification of the former is not easily defined. Moreover, cyber crises will cause direct strategic implications, generating a strong sense of urgency and affecting external stakeholders, possibly threatening to cause long lasting damage to the company's reputation and attracting external scrutiny through (inter)national media exposure.

Because of the nature of the service that the CERT offers, as well as ransomware being the most frequent type of engagement, the majority of the instances in which the team is involved can be identified as cyber crises. The impact on the business is often so high that if the systems are not rapidly recovered the organisation risks going out of business. Furthermore, the experience of the team is that in most of the cases the client does not have a dedicated Crisis Management Plan (CMP) and consequently there is not a formal distinction between a cyber incident and a cyber crisis at a management level. This is not to say that there is no difference between a cyber incident and a cyber crisis, but rather to indicate the absence of a formal handover between the two. Having a CMP and a crisis management process more broadly defined at company level would have an impact on the CERT activities as well. One interviewee stressed how it changes the role of the team as a whole, which instead of being considerably involved in managing the crisis, diminishes to just being in charge of its digital part. It ensures that all the relevant stakeholders are involved at the right time, substantially speeding up the process and allowing for

a more mature and proactive management of the crisis.

Lastly, the interviewees pointed out how although cyber crises manifest suddenly, they often do offer early warning signals. Taking ransomware cases as an example, the attackers have to first get a foothold into the infrastructure and then gain access to the advantage point needed to successfully deploy the ransomware to the target infrastructure. Traces of such activities, which can range from the use of specific adversary tools to the creation of accounts with administrative rights, are logged and can be detected. Security monitoring can therefore detect the adversary activity and give the organisation an opportunity to avert the crisis by timely responding to the incidents that lead to it. However, as pointed out in the previous section, a lack of security monitoring has been identified for the client organisations, leading attackers' activity to go undetected until its conclusive stages and to directly manifest as a crisis.

3.3 Discussion

The interviews have contributed with two significant results that required to adjust the strategic direction of the research. Firstly, in the vast majority of the cases where the team has intervened, the client did not have a crisis management plan in place. Although this result was not expected, supporting evidence that indicates a low level of crisis formalisation, and consequently of crisis management plan formulation, has been found in [38]. The lack of crisis management plans considered in combination with the highly disruptive nature of ransomware attacks, which represent the majority of the cases for which the CERT gets engaged, contribute to the absence of a formal transition from incident to crisis management for the considered cases.

Moreover, the interviewees have also highlighted how the very low incidence of clients with a security monitoring solution in place often prevents the organisation from detecting the signs of the security incidents that eventually lead to the manifestation of the cyber crisis. This suggests that a transition from incident to crisis is present when considering the sequence of events that constitute the attack. However, this is not reflected at a management level because such events are not monitored, and therefore it only becomes visible to the organisation during the manifestation of the crisis. The common reason behind both findings has been consistently identified with the lack of a security management strategy defined at an organisational level, which is indicative of a low security maturity more broadly.

The interviews have also highlighted how, in order to both gain a deeper understanding on the impact of the attack and to prioritise the recovery work, the activity of mapping the business processes of the client organisation to its IT infrastructure requires cooperation between the IT and the management team of the client. This

activity has been found to be at times cause of friction between the two teams as the IT personnel is often very technical in nature and therefore not proficient in supporting this activity. In this regard, although not commonly in place, having punctual documentation on the infrastructure has been identified a factor that facilitates this activity.

Lastly, another aspect that was covered in the interviews considered how the members of the team discern a cyber incident from a cyber crisis. Notably, the responses can be identified as consistent with what is presented in [27]. In particular, the interviewees have highlighted how cyber incidents can be solved fairly quickly, by following routine procedures and do not affect business operations in a significant way. Cyber crises will instead cause direct strategic implications, generating a strong sense of urgency and affecting external stakeholders, possibly threatening long lasting damage to the company's reputation and attracting external scrutiny through (inter)national media exposure.

Chapter 4

Ransomware at Maastricht University

This chapter analyses the cyber crisis that Maastricht University (UM) underwent in December 2019 as a result of a ransomware attack. The objective is that of exploring a real case to support the consideration made in Chapter 3 while suggesting how security monitoring could have averted the cyber crisis by detecting the incidents that led to it, therefore allowing for corrective action. The chapter is structured as follows: Section 4.1 frames the cyber crisis by outlining the scenario in which it developed; Section 4.2 outlines the timeline of events that lead to the final manifestation of the ransomware attack; Section 4.3 discusses how the adversary activity was detected in multiple instances and a response to it could have averted the crisis, and it outlines how UM responded to the cyber crisis.

4.1 Scenario

On the evening of December 23^{rd}, 2019, Maastricht University was severely hit by a ransomware attack that resulted in the encryption of 267 Windows servers and in the complete disruption of daily operations. The attack manifested suddenly, completely getting the organisation by surprise and immediately posing direct strategic implications. Among the affected machines were in fact systems that supported the whole business environment and were critical for daily operations – such as domain controllers, exchange servers, file servers with research and management data as well as some of the backup servers [39]. This immediately generated a substantial sense of urgency towards finding a solution that would at least restore the essential business processes in a short time frame; the complexity of the attack and the exceptional magnitude of its implication soon hinted however to a longer resolution time. Few hours later, the organisation closed connections to and from the Internet to exclude the possibility that the attacker could cause additional disruption. The university contacted an external CERT to help structure a recovery plan, which sent

a team of specialists on site the following day. Quickly, the university also opened communications with the Team High Tech Crime of the National Police, the National Cyber Security Centrum, and SURFcert [40]. The forensic analysis that was conducted by the external emergency response team concluded that it would not be possible to sufficiently restore the systems from the backups as they were also largely encrypted. Therefore, UM decided to pay the ransom that was demanded by the attacker – and which amounted to 30 Bitcoins[1] – in order to receive the decryption key [41].

The attack resulted in an organisational crisis that severely tested the resiliency of the university in the very short time frame that preceded the exam sessions for its 18,000 students. The crisis drew significant media attention, both national and international, and it took at least two weeks before the university could get back to some degree of normalcy [42], [43]. On February 5^{th}, 2020, Maastricht University held a symposium that provided a more detailed insight into the cyber attack, and addressed broader cyber-related issues, such as digital security in the public sector [44]. Moreover, on that date the university also published a public version of the forensic report that was drafted after the technical investigation was concluded [39].

4.2 Attack Timeline

On October 15^{th}, 2019, a UM employee received a phishing email – reported in Figure 4.1 – that contained an external link to an Excel document. The employee downloaded and opened the file, triggering a hidden macro that downloaded and silently installed the SDBbot malware on the workstation. SDBbot [45] belongs to the Remote Access Trojan (RAT) family of malware, and allowed the attacker to remotely control the infected system. A similar email was received the next day by five other UM employees - one of them opened the attached file, which in turn downloaded and installed SDBbot on that system as well. This allowed the attacker to establish a first foothold into the infrastructure, from which he was then able to initiate a sequence of malicious operations.

Between October 17^{th}, 2019, and October 19^{th}, 2019, the attacker succeeded in compromising four servers within the UM infrastructure. Although the limited amount of forensic traces do not provide a definite answer on how the attacker managed to compromise the machines, three of the four servers were found to be vulnerable to EternalBlue - leading the investigators to believe that the attacker leveraged that unpatched vulnerability. EternalBlue is a zero-day exploit that was allegedly developed and covertly used by the NSA until it was leaked in April 2017 by The Shadow

[1] About €200,000 considering the exchange rate at that time

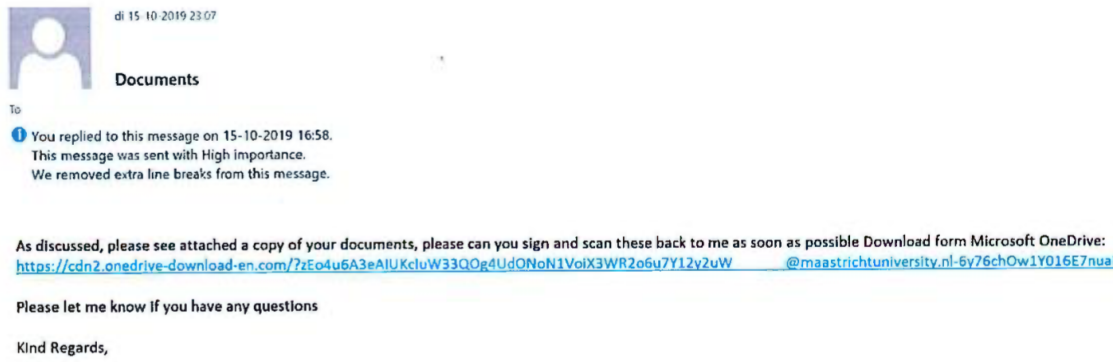
Table 4.1: Attack timeline based on [39]

Date	Action
15-10-2019 16:56	The Excel file linked in the first phishing email is opened and SDBbot is installed on the workstation.
16-10-2019 12:52	The Excel file linked in the second phishing email is opened and SDBbot is installed on the system.
24-10-2019 11:41	Windows defender detects and removes PowerView.
21-11-2019 13:19	The attacker accesses an account with domain administrator rights and logs into a domain controller.
19-12-2019 16:35	McAfee detects multiple times the attacker's activity.
23-12-2019 17:55	The attacker prepares to mount the attack; McAfee detects and removes the ransomware deployment tool.
23-12-2019 18:26	The attacker starts the ransomware deployment.
23-12-2019 18:52	267 Windows servers are encrypted.
30-12-2019 13:50	UM receives the decryption key from the attacker after having payed the ransom.

Brokers [46]. Since its release, this remote code execution exploit has become extremely popular as it is not only extremely severe but it also affects all versions of the Windows operating system. EternalBlue constituted in fact one of the main factors of success of the 2017 NotPetya ransomware campaign that was outlined in Chapter 1. Nevertheless, it is worthwhile to highlight that Microsoft had been informed about the vulnerability before its disclosure and had released a security update that patched it completely on March 14^{th}, 2017 [47].

During the following five days, the attacker performed various activities with the intent of mapping the infrastructure and of gaining better network situational awareness. On October 24^{th}, 2019, PowerView - one of the tools that was being used by the attacker - was detected and deleted by Windows Defender. The defensive action was logged by the application, which accurately reported the detection of "HackTool: PowerShell / PowerView.A". After a period of inactivity, forensic traces show that on November 21^{st}, 2019, the attacker resumed his operations and managed to get access to an account with domain administrator rights. With the privileged account he was then able to log into one of the domain controllers. At this point, the attacker had access to the system with the higher privileges (domain controller) as the user with the highest rights (domain administrator).

On December 19^{th}, 2019, adversary activity is again detected on multiple sys-


di 15-10-2019 23:07

Documents

To

You replied to this message on 15-10-2019 16:58.
This message was sent with High importance.
We removed extra line breaks from this message.

As discussed, please see attached a copy of your documents, please can you sign and scan these back to me as soon as possible Download form Microsoft OneDrive:
https://cdn2.onedrive-download-en.com/?zEo4u6A3eAlUKcluW33QOg4UdONoN1VoiX3WR2o6u7Y12y2uW @maastrichtuniversity.nl-6y76chOw1Y016E7nua

Please let me know if you have any questions

Kind Regards,

Figure 4.1: Phishing email that was received on October 15^{th} [39].

tems. McAfee Enterprise Endpoint Security detected and deleted multiple instances of both adversary tools CobaltStrike and Mimikatz. Having access to admin credentials the attacker was however able to switch McAfee to observer mode - meaning that the antivirus would detect and log the malicious activity but it would not block it - and redeployed the tools. On December 23^{rd}, 2019, the attacker started the preparations necessary to deploy the ransomware; during the activity, McAfee detected and removed the ransomware deployment tool. However, similarly to what he had previously done, the attacker was able to turn McAfee into observer mode and to redeploy the tool.

Eventually, on December 23^{rd}, 2019, at 6:26pm the attack was run from the compromised servers and few minutes later, at 6:52pm the 267 Windows servers which included domain controllers, exchange servers, file servers with research and management data as well as several backup servers were encrypted.

4.3 Discussion

Although the lack of maturity in the security posture held by Maastricht University undoubtedly acted as an enabler for the attack, the previous section highlights how the attacker was able to stay in the infrastructure for a quite significant period of time without being detected. Ten weeks elapsed between the moment when the attacker first delivered the phishing emails and got into the infrastructure, and the moment in which the ransomware was actually deployed. The previous section showed indeed that traces of the intruder were present in the system logs already on October 24^{th}, 2019, when Windows Defender detected and removed PowerView, one of the tools used by the attacker to gain situational awareness on the network. Moreover, during the attacker's preparations to deploy the ransomware in December, McAfee detected multiple instances of adversary tools as well as the ransomware deployment tool itself. Had a monitoring process been in place, the evidence indicating the malicious

Figure 4.2: Google suggested queries when searching for “universiteit maastricht”.

activity would have been detected, giving UM the opportunity to apply corrective measures that would have averted the crisis. Therefore, what may have looked like a sudden and unpredictable event to the external observer can instead be identified as the final manifestation of a series of incidents that had started two months in advance. While adequate security measures might have prevented the attack from happening in the first place, the lack of security monitoring led what started as a security incident to slowly escalate during an extensive period of time into a full blown cyber crisis - confirming and further reinforcing what has been highlighted in Chapter 3.

One of the earliest actions that have been performed by the external incident responders has been that of aiding the university in structuring the crisis organisation, as well as advising and engaging a communication specialist. On December 24^{th}, 2019, UM published an update on its website revealing that it had fell victim of serious cyber attack; moreover, during the period between December 27^{th}, 2019, and January 10^{th}, 2020, the university published on its website daily updates regarding the recovery progress as well as recommendations for both students and employees [44]. This allowed the university to gain a role as the main source of information, therefore achieving a significant degree of control over the narration of the events. Additionally, not only the daily updates contained detailed information on the point of contacts, but different point of contacts were presented to different audiences and kept current with each update.

The cyber crisis undoubtedly scratched the reputation of the university, which ranks in the top 250 universities worldwide [48]. Although the attack occurred fairly recently and therefore it is arguably too early to observe any long lasting consequences on UM’s reputation, it is exemplary to ascertain how the first two suggestions featured by a Google search for the keyword “universiteit maastricht” are both relative to the cyber attack (see Figure 4.2).

To conclude, on February 5^{th}, 2020, UM held the “cyber attack symposium” in which the university provided a deeper insight into the cyber attack. Moreover, during the event the lesson learnt were addressed and a public version of the forensic report was released in light of transparency [44]. This indicates how the university has attempted to turn the cyber crisis into an opportunity, not only to improve its security posture but to also showcase an example of resiliency. Furthermore, publicly sharing the details, and the complete sequence of events that led to the cyber attack gave other organisations an opportunity to improve their security posture. Further promoting awareness on the serious impact that a cyber crisis can bring about, not only on the digital domain but also on the business itself.

Chapter 5

Cyber Crisis Management - Case

This section reports the most relevant considerations that have emerged by conducting a semi-structured interview with a senior incident response coordinator of Northwave's CERT. The objective of the interview was that to confirm the findings presented in Chapter 3 and Chapter 4, as well as of investigating which tasks and which challenges become most prominent when managing cyber crises. This has been done by examining a concrete case while also engaging in more comprehensive considerations matured on the base of extensive experience in analogous cases. Therefore, Section 5.1 presents the scenario describing a specific instance of a cyber attack and discusses whether early signals could have been detected; while Section 5.2 considers the activities relative to cyber crisis management, both in this specific case and more broadly in similar cases. Moreover, Company A has been used as a pseudonym instead of the real name of the company to preserve its anonymity. The same method that has been presented in Chapter 3 has been used to structure the present interview – for a detailed description the reader can refer to Section 3.1. For completeness, the integral interview guide is provided in Appendix B.

5.1 Scenario

During the month of June 2020, Company A was severely hit by a ransomware attack that affected more than three quarters of its infrastructure, significantly hindering daily operations and instantly leading the organisation to a state of crisis. The company, which is active in the manufacturing of industrial machinery, operates in 10 countries worldwide and has a workforce of around 2,000 employees. Forensic investigations showed that the attacker first got a foothold into the infrastructure about six weeks before the ransomware was deployed – this was most probably done by performing a brute force authentication attack against a VPN account. The

encryption process took place over night, a strategy commonly used by attackers as employee activity is minimal during the nightly hours and therefore the chances of direct detection become slimmer. The attack was detected the next morning, when employees from the early shift could not access the files stored on the corporate server, quickly leading the organisation to realise that it had been hit by a ransomware attack.

To the external observer, the crisis manifested suddenly, without giving any early warning signal nor possibility for preparation. However, it was stressed during the interview that if the right measures would have been in place, a number of suspicious activities that would have given an indication of the attacker entering and moving through the infrastructure could have been detected. This would have prevented the crisis by allowing for a proactive treatment of the incidents that led to it. Had security monitoring been in place, the organisation could have been notified, for instance, about about the high number of login attempts, which would have allowed for corrective action.

Moreover, once they gain access to the target infrastructure, cybercriminals often use similar sets of tools to explore the environment, get access to specific target systems and obtain the necessary privileges. Mimikatz and Cobalt Strike are two very popular tools that are often used. The first allows attackers to steal account credentials and escalate privileges, while the second is often used to set up a covert command and control infrastructure to be later used for the ransomware deployment. Antivirus solutions most often detect and prevent the usage of such tools; however, having gained the necessary privileges, attackers are often able to disable them and redeploy the applications – as it was also highlighted in Chapter 4. Nonetheless, in the context of security monitoring, the deactivation of an antimalware solution would represent an alarming activity that would give the organisation a clear indication of possible malicious operations.

Furthermore, the interviewee stressed how most of the times the mentioned activities are present in the logs (or at least have been, in case of a short log retention period) – which is why it is then possible to reconstruct the events by the means of a forensic investigation. What lacks is the implementation of a process of monitoring that is able to analyse the generated logs in order to spot anomalies and deviances from the regular behaviour of the infrastructure. This is a consideration that not only applies in this specific case, but that is also applicable to the vast majority of the cases in the CERT portfolio. Consequently, in most of the ransomware incidents for which the team is engaged the first sign of the attack that the client detects is the ransomware itself.

5.2 Crisis Management

This section reflects the findings of the second part of the interview, which focused on analysing the challenges that emerged during crisis management in both the case of Company A and, more in general, in analogous cases. In particular, the questions have been structured considering part of the tasks that leaders are called to perform during crises presented in Section 2.5, as well as elements from the crisis management process presented in Section 2.4.

5.2.1 Preparation

Structuring a Crisis Management Plan is arguably the most important activity to be performed during the prepare phase outlined in [27]. The plan makes sure that the organisation considers and prepares for the activities that will have to be performed during a crisis, adding a structural level that will prevent the organisation from falling into a chaotic state when under pressure.

When Northwave arrived on site, Company A had set up the crisis organisation and had already formed a Crisis Management Team (CMT), which encompassed people from IT, legal, information security, marketing & communication, and management. This allowed for a holistic approach to the management of the crisis which leveraged figures from different areas of the business to achieve a comprehensive view on the implications that the crisis brought about. Although the previous could indicate that the organisation was following a formally defined crisis management plan, the interviewee was not able to confirm it. In this regard, however, as already highlighted in Chapter 3 and further confirmed by the interviewee, it is extremely rare that the organisations that engage Northwave's CERT do have a formally defined CMP.

Nevertheless, the interview highlighted that when organisations do have a CMP in place it becomes very clear what are the roles that must be present in the CMT, who are the specific people designated to cover such roles, and what are the responsibilities that the different members of the CMT will have to cover. During a crisis, having a CMP assists organisations with giving structure, guidelines on how actions should be documented, frequency of meetings and ensures that all the relevant stakeholders are involved. As the interviewee puts it, having a crisis management plan will allow the organisation to completely focus on managing the crisis without having to go through the time consuming process of creating procedures at the same time.

One of the main drivers behind the tendency of not having crisis management plans has been identified with the attitude of many organisations of failing to ac-

knowledge that cyber crises are a reality that could affect any business, and regardless of the effectiveness of the security controls that are put in place – as it is also remarked in [27]. Often, corporate management is in fact not familiar with how criminals operate in cyberspace and therefore engage with the assumption that cybercriminals would not target their organisation as it has nothing valuable to offer them. This is a consideration that fails to capture how this segment of cybercriminals, which is driven by a mere financial motive, does not target organisations because of the business they conduct, but rather because they are found to be digitally vulnerable. The company is then only considered in financial terms, in order to get a sense of how profitable an attack would be, weighing how much time and effort the attack would require against the amount that can be asked as ransom. This leads management to a perception of the risk which is often not in line with the threat landscape.

Another driver has been identified in organisations not fully realising how much their business relies on the underlying IT infrastructure, and consequently, how much a critical disruption in the infrastructure would impact its ability to operate. This is also driven by the unique characteristics that cyber attacks offer and which have been outlined in Section 2.3.1. It may not be straightforward to realise that conversely to traditional criminals, cybercriminals can perpetrate the malicious activities directly from a foreign country and with a high degree of anonymity; or that a cyber attack can severely affect all of the locations in which the organisation operates at the same time.

5.2.2 Early Recognition

The central element of exploration present in this phase was directed to understand whether there had been warning signals that could have indicated adversary activity leading to the cyber crisis, and whether measures where in place to detect and act on those signals. The discussion revolved around two main topics.

The first one relates to what has been discussed in Section 5.2.1 and considered how a significant portion of the management is not familiar with the way cyber criminals operate as well as how the organisation extensively relies on the underlying IT infrastructure. This can lead companies to the conclusion that they have a low chance of being hit by a cyberattack – resulting in a feeble security posture which prevents the organisation from detecting and acting on early warning signals.

The second one relates instead to what has been discussed in Section 5.1. This kind of cyber attacks often leave traces of their activity in the various systems that they get in contact with. However, in most cases there is not a process in place that would allow the clients to detect anomalies and act upon them. For most of the client

companies, indeed, although an enabler IT is not the core business. Consequently, the IT department is often modest in size and responsible for managing an extensive list of priorities. Therefore, if a structured approach to cyber security management is not set at an organisational level and endorsed by the top management of the organisation, IT security is going receive little attention – even though the technical team may see its value and, to a certain extent, understand the related risks.

In the case of Company A however, the client had already begun a programme that aimed at improving its cybersecurity posture. Nevertheless, although some security measures had already been taken, the programme was still not extensively developed and solutions like security monitoring were not implemented because of budget constraints. This allowed the attacker to go undetected for a period of six weeks. Period during which he was able to understand what the crown jewels and the critical resources of the company were, in order to make sure that the attack would cause the highest possible level of disruption – which would compel the company to pay the ransom amount. This way of proceeding is consistent with what the team witnesses in analogous cases: cybercriminals are confident of not being detected and therefore really take the necessary time to prepare the attack in a very well organised manner. As stated by the interviewee: "*They know your business, how much you earn, how valuable your data are, how long you will survive without the decryption key. It is a very solid machine.*"

5.2.3 Sense Making

Although Chapter 2 highlighted how understanding the magnitude of a cyber incident is one of the challenges identified in the incident management process, the extent of the consequences of the cyberattack was rather clear in this case. The ransomware resulted in a very extensive disruption that led to more than three quarters of the company not being able to operate, posing the clear risk of permanent damage that could potentially take the client out of business if not promptly resolved. New material could not be ordered, access to the company's CRM system was impossible, there was no telephony and no emails for a certain period of time – the whole infrastructure was significantly impacted. This reflects the immense disruptive potential that cyber attacks can have on a business, spotlighting how the consequences are not limited to the cyber domain but extensively impact the physical domain too. Moreover, as it was also previously pointed out, it is only through such disruptive attacks that most companies realise how much the business relies on its IT infrastructure.

As highlighted in [26], making sense of a crisis situation is a very challenging task due to the element of uncertainty and ambiguity that characterises organisational

crises. However, two factors contributed in facilitating the sense making activities in this case. The first, which is also one of the reasons why the attack was so effective, is that Company A had a rather flat network design in place; this made it easier to trace the attacker's activity as well as to understand which resources could have been impacted. The second factor is that Company A had developed a very well structured Configuration Management Database (CMDB), of which an offline copy was incidentally done the day prior to the attack. A CMDB acts as a digital warehouse, which stores information about the hardware and software assets that constitute the IT infrastructure. Moreover, it outlines how different systems are configured and connected together, allowing to easily map component relationships and interdependencies. This allowed for a more efficient and effective analysis of the impact as well as it aided the investigation of the root cause.

Another significant activity that relates to the previous was that of prioritising what part of the business had to be restored first. In this case, Company A had a fine understanding on how the business was mapped to the IT infrastructure, so once the parts of business that needed to be restored first were prioritised, it was then relatively straightforward to know what systems needed to be restored. This was partly due to the presence of the well structured CMDB previously mentioned.

Although it represented a favorable factor in this case, having a good overview on the company's infrastructure is something that is rarely seen in the companies for which Northwave's CERT gets engaged. Consequently, it is common that clients have a really good perception on which business processes should be resumed with a higher priority, but then encounter significant challenges when having to map them on the IT infrastructure – which can occasionally lead to internal friction.

Lastly, cyber attacks are a phenomenon of technical nature, which however cause an indisputable impact in terms of business. Therefore, delivering the management with a general understanding of what the attack is, what it entails, and what are the steps that need to be taken in order to recover, is something that is not straightforward to achieve. In this case, the incident response coordinator acted as the expert on the incident to convey how the attack had happened and what the recovery process looked like. He cooperated with the head of IT of Company A which acted instead as the business expert and covered the responsibility of explaining how the attack connected to the business, what the impact was and motivating the chosen priorities. This combination worked finely as it leveraged the ability of both individuals to bridge the gap in technical knowledge with effective communication, creating a clear link between the digital and the business aspect of the crisis.

5.2.4 Decision Making

One of the most prominent decisions that had to be taken during the management of the crisis was whether or not to pay the ransom. To mature a decision, the first element to determine is whether or not unencrypted backups are available, and if so, whether they are sufficient not only to restore the company operations but also to do it in a financially sound time frame. This can be approximated by weighing the financial amount demanded as ransom against an estimate of the financial loss experienced in the time needed to perform a backup recovery. Moreover, considering that interacting and negotiating with the attacker to get the decryption key requires time, and that - depending on the size and structure of the company - a period of at least five day is needed to restore a significant part of the company's operations, this has to be an early decision.

Once the previous is established, there are at least another two key aspects that must be considered. The first is an ethical consideration. The business model of the cybercriminals relies on victims paying the ransom in order to survive. In this sense the interviewee highlighted how attackers rarely behave in hostile terms and instead often show an attitude towards cooperation. It is indeed in their best interest that the process of payment and decryption goes as smoothly as possible. This raises trust in the business model, leading future victims to be more incline to pay the demanded amount. Therefore, a decision to pay the ransom not only supports but also aliments the criminal business model.

In this regard, the Dutch National Cyber Security Center advises organisations that fall victim of ransomware attacks not to pay the demanded amount: "*Paying the ransom also preserves a business model; it encourages cyber criminals to use ransomware, as it is a profitable undertaking. Cyber criminals will then continue their activities and seek out new ways of exploiting systems, resulting in more infections, more victims and more harm to society*" [49, p. 3]. However, although this is good in principle, the reality tends to be more complex. The financial difference between restoring the infrastructure by paying the ransom or by rebuilding it completely can be very substantial. The City of Atlanta, for instance, fell victim of a ransomware attack in 2018 and refused to pay the ransom that was set to 51,000$. This resulted in an expense of 17M$ necessary to rebuild its network [50]. Although the choice of not alimenting the business model in spite of the significant financial losses can be regarded as exemplary, it does not represent a viable solution for many entrepreneurs. This is, for instance, the case of the ransomware attack that affected a Dutch logistic company in February 2020, and for which Northwave was engaged. Although the owner had the clear intention not to pay the criminals, he soon realised that paying would be the only solution to avoid bankruptcy. Rebuilding the system and rescanning the stock would take at least two weeks: "*Dan konden we onze contractuele*

verplichtingen niet nakomen en zouden we al vrij snel richting faillissement gaan. We moesten onderhandelen." [Then we could not meet our contractual obligations and we would soon go into bankruptcy. We had to negotiate.] [51].

Furthermore, the CERT has observed a new trend over the first half of 2020, where the attackers exfiltrate sensitive data before running the encryption process – consistently to what has been reported in [52], [53]. This is done in order to have more leverage; with such data the attacker can in fact threaten the organisation to publish it if the ransom is not payed. Organisation become then very prone to pay as the implications that would arise from the combination of the financial damage and the disclosure of sensitive information would be very substantial. Consequently, understanding if sensitive information has been exfiltrated is an additional consideration of extreme importance. In this case, forensic evidence could only indicate that the attacker had accessed certain folders and that traces of exfiltration were present, however it was not possible to determine exactly what information was exfiltrated. Therefore, it could only be concluded that specific folders had been accessed and that a subset of the information contained in such folders had been exfiltrated, although it was not possible to establish which. Once it became clear that information was exfiltrated, the client – which was debating on whether or not to pay the ransom as it seemed that part of the infrastructure could be restored from backups – quickly matured the decision to pay the ransom.

Chapter 6

Conclusions

The present research aimed at investigating what factors become of relevance when considering the transition between cyber incident management and cyber crisis management in a corporate environment (RQ 1). A first exploratory step has been performed in Chapter 3 by conducting semi-structured interviews with members of Northwave's Computer Emergency Response Team (CERT). The team gets often engaged as an external resource by companies that fall victim of severe cyber attacks and for which they do not possess the people, the resources or the capacity necessary to autonomously resolve. The aim was that of leveraging first hand experience to investigate how companies deal with managing the cyber crisis in the context of such engagements. Nevertheless, the interviews have highlighted that the vast majority of the engagements do not feature a formal transition from cyber incidents to cyber crises. The latter manifest suddenly and with no early warning signs to the client organisations. However, this is not to say that there is no transition between the two but that rather the transition is not observed. A lack of security monitoring has been identified as the key factor that prevents client organisations from identifying and reacting to the sequence of cyber incidents that eventually leads to the cyber crisis.

To further support this finding, Chapter 4 explored the cyber crisis that Maastricht University experienced in December 2019 as a result of a ransomware attack. The analysis, based on the data published in the forensic report of the attack, showed how although a feeble security posture acted as an enabler, the lack of adequate security monitoring allowed the adversary activity to go undetected for an extensive period of time. Since the attacker gained a foothold in the target infrastructure, multiple instances of malicious applications that were used to prepare the attack – including the ransomware deployment tool – were detected and logged by the antivirus solution that was running on the compromised systems. However, the absence of a process in place to identify and react to such detections led what started as a cyber incident to materialise as a cyber crisis ten weeks after the initial

compromise, further highlighting how – although not observed – a transition between the two took place.

The above mentioned consideration was further confirmed through the analysis of a ransomware case for which Northwave's CERT was engaged in June 2020. The discussion, presented in Chapter 5, highlighted how security monitoring could have averted the crisis by identifying the sequence of cyber incidents that led to it and therefore allowing for corrective action. Moreover, the interview has highlighted how one of the main drivers that lead client organisations not to have a prominent security posture – and consequently, a security monitoring process in place – can be identified in a misplaced perception of the risk related to cyber attacks. This has been reconducted to the clients' lack of awareness on how this segment of financially motivated cybercriminals operates, as well as on how reliant modern companies are on the underlying IT infrastructure. Furthermore, the interviews that have been conducted in Chapter 3 and Chapter 5 have also highlighted how for the vast majority of the cases where the team is engaged the client does not have a crisis management plan in place. Although this result was not expected, supporting evidence that indicates a low level of crisis formalisation, and consequently of crisis management plan formulation, has been found in [38].

Another topic that the research set to investigate considered at what point a cyber incident turns into a cyber crisis (RQ 1.a). A direct exploration of the transition between the two, which would have provided a substantial insight on how the transition point is identified, has not been possible. As mentioned above, our investigation revealed the shared absence of a security monitoring process as well as of a formal crisis management plan. This inherently prevents the organisation from detecting the incidents that lead to the crisis, and consequently the transition between the two. Nevertheless, the interviewees have been probed regarding their interpretation on the difference between the two in Chapter 3. The responses have highlighted how cyber incidents can be solved fairly quickly, by following routine procedures and do not affect business operations in a significant way. Cyber crises will instead cause direct strategic implications, generating a strong sense of urgency and affecting external stakeholders, possibly threatening long lasting damage to the company's reputation and attracting external scrutiny through (inter)national media exposure. This result has been found to be consistent with what is presented in [27]. Moreover, the scale of the impact and its direct implications on the ability to perform the core business activities has been consistently identified as the main factor that can be used to discern between the two. However, we argue that this may be influenced by ransomware attacks being the most common form of engagement, as they significantly impact the availability of the victim's core assets.

Lastly, the research investigated what aspects do require cooperation between

the incident response team and the crisis management team when transitioning to a cyber crisis (RQ 1.b). The exploratory steps that have been performed in Chapter 3 and Chapter 5 have highlighted how the activity of mapping the business processes of the client organisation to its IT infrastructure – in order to both gain a deeper understanding on the impact of the attack and to prioritise the recovery work – requires cooperation between the two teams. This activity has been found to be at times a cause of friction between the client's management team and the client's IT team – often very technical in nature and therefore not proficient in supporting this activity. In this regard, having punctual documentation on the infrastructure and a well structured CMDB repository have been identified as facilitating factors. Nevertheless, it was stressed how clients do only rarely have them in place during the engagements.

6.1 Recommendations

Although cyber crises appear to arise suddenly, the present research showed how they instead materialise as the last manifestation of a sequence of cyber incidents. The vast majority of the client organisations have in fact been identified not to have a security monitoring solution in place. This prevents them from observing the transition that leads cyber incidents to escalate to cyber crises and, consequently, from treating them in order to avert the crisis. Therefore, we advise organisations to implement a security monitoring solution which would allow them to timely react to cyber incidents before they escalate to crisis magnitude. However, we want to stress that this should not be an isolated effort but it should rather be part of a broader cybersecurity strategy defined at a corporate level and endorsed by senior management. In particular, the NIST cybersecurity framework [18] outlined in Chapter 2 represents a valid approach to develop a well structured cybersecurity strategy. Furthermore, we recommend to invest in the design and implementation of a cyber crisis management plan as part of the security strategy. The plan makes sure that the organisation considers and prepares for the activities that will have to be performed during a crisis, adding a structural level that will prevent the organisation from falling into a chaotic state when under pressure. Lastly, one of the challenges that are often encountered during the recovery from a cyber attack is that of translating the business processes to the IT infrastructure. In this sense, we recommend and encourage organisations to develop and maintain punctual documentation on the IT infrastructure. Punctual documentation, and CMDB solutions in particular, have in fact been identified as factors that facilitate the investigations as well as the analysis of the root cause by the interviewees – allowing for a faster and more efficient process of recovery.

6.2 Limitations

The present research offered a first exploratory insight on the transition from cyber incidents to cyber crises, the results have however to be interpreted in the context of the following limitations. Firstly, convenience sampling was used to identify the population surveyed throughout the research. The topic of analysis has consequently been observed from the single perspective of Northwave's CERT. Therefore, extending the scope of the research by surveying multiple CERTs – possibly across different countries – would introduce a sample more representative of the entire population and hence increase the external validity of the study.

Secondly, the topic of analysis has been observed from the perspective of a CERT. We argue that because of the nature of the service that it offers, companies that engage with the CERT would intuitively be representative of a population of organisations with a lower security posture, consequently introducing an observation bias. Therefore, performing a similar exploratory approach in the context of more security mature companies would possibly yield different results, which could extend the validity of the present research and which we identify as an opportunity for future research.

Lastly, ransomware attacks, in which the attacker is motivated by a mere financial interest, have been identified in Chapter 3 to represent the vast majority of the engagements. This inherently lead the discussion to focus on such cases, restricting the area of exploration. In this regard, it should be also considered that Northwave's partnership with an insurance company represents the predominant channel with which client organisations come into contact with the CERT for this kind of engagements. Therefore, a strategic preference of the insurance company to focus on a specific segment of target companies could represent an external element of bias.

Furthermore, that of acquiring primary data in the field of information security research is a well know challenge. Kotulic and Clark highlight in fact how *"information security research is one of the most intrusive types of organization research, and there is undoubtedly a general mistrust of any 'outsider' attempting to gain data about the actions of the security practitioner community"* [5, p. 604]. We identify this challenge to become even more prominent when wanting to investigate cyber incidents/crises. Such events, in fact, do not become public in most cases – and when they do, only limited information is publicly shared. Therefore, cooperation with affected companies poses a clear confidentiality challenge which can only be overcome when an extremely high level of trust with the researcher is present.

6.3 Future Work

We consider the present thesis to be the base on which further studies can be developed, opening up to different research opportunities. We propose that a similar study could be conducted by taking advantage of a different point of observation than that of a CERT. This would allow to consider organisations with different levels of security maturity as well as different threat scenarios. In particular, we expect more mature companies to have a security monitoring process in place, therefore offering visibility into the process of escalation from incident to crisis and to allow for a direct exploration of the transition between the two. At the same time, however, mature companies will be less likely to be hit by cyber crises, therefore making such cases more rare to identify.

Performing a case study within a company that suffered a cyber crisis has been identified as another opportunity for further studies. Conducting the research as part of the company would inherently create a higher level of trust between the organisation and the researcher. This would result in easier and more complete access to involved people, resource, data, and documentation. We suggest that semi-structured interviews could be employed as data collection method based on the model developed in the present research. The exploration can build on the present research and encompass an analysis of both the process of transition from incident to crisis and of cyber crisis management itself. Furthermore, it must be noted that a single case study design would reduce external validity. Nonetheless, considering the difficulty to get primary data in this context, we deem this to be a reasonable approach.

Lastly, the transition from incident to crisis does not only represent a technical handover, but it firmly relies on the human component to continuously assess the situation and to take decisions – inherently becoming prone to cognitive biases such as sunk cost bias and confirmation bias [54]. Moreover, escalating an incident can be perceived as an admission of failure or can be identified as a potential threat to job stability – leading employees to be averse to activate the escalation procedure [55], [56]. Additionally, phenomena such as groupthink [57] and risky shift [58] have been showed to influence the behaviour of individuals in a group, and are expected to be present in this context as well. Therefore, we identify the analysis of the process of escalation between cyber incidents and cyber crises from a behavioural standpoint as an opportunity for future research.

Bibliography

[1] Maersk. (2017) Cyber attack update july 3rd. [Online]. Available: https://twitter.com/Maersk/status/881927414955352064

[2] A. Greenberg. (2018) The untold story of notpetya, the most devastating cyberattack in history. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[3] D. Pretty, "Reputation Risk in the Cyber Age," Pentland Analytics, Tech. Rep., 2018.

[4] PwC, "Global Crisis Survey 2019," 2019. [Online]. Available: https://www.pwc.com/gx/en/services/advisory/forensics/global-crisis-survey.html

[5] A. G. Kotulic and J. G. Clark, "Why there aren't more information security research studies," *Information & Management*, vol. 41, no. 5, pp. 597–607, 2004.

[6] S. Kuipers and N. H. Welsh, "Taxonomy of the crisis and disaster literature: Themes and types in 34 years of research," *Risk, Hazards & Crisis in Public Policy*, vol. 8, no. 4, pp. 272–283, 2017.

[7] Northwave, "Northwave. intelligent security operations," 2020. [Online]. Available: https://northwave-security.com/en/

[8] Scopus, "Welcome to scopus." [Online]. Available: https://www.scopus.com/home.uri

[9] J. Webster and R. T. Watson, "Analyzing the past to prepare for the future: Writing a literature review," *MIS quarterly*, pp. xiii–xxiii, 2002.

[10] I. A. Tøndel, M. B. Line, and M. G. Jaatun, "Information security incident management: Current practice as reported in the literature," *Computers & Security*, vol. 45, pp. 42–57, 2014.

[11] Allianz, "Allianz risk barometer. identifying the major business risks for 2020," 2020. [Online]. Available: https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

[12] K. Zetter, “An unprecedented look at stuxnet, the world’s first digital weapon,” Wired, 2014. [Online]. Available: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

[13] N. Perlroth, “In cyberattack on saudi firm, u.s. sees iran firing back,” The New York Times, 2014. [Online]. Available: https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html

[14] World Economic Forum, “The global risks report 2018. 13th edition,” 2018. [Online]. Available: https://www.weforum.org/reports/the-global-risks-report-2018

[15] D. Dimov, “Malware-as-a-service,” Infosec Institute, 2017. [Online]. Available: https://resources.infosecinstitute.com/malware-as-a-service/

[16] Zurich, “Information security and cyber risk management,” 2018. [Online]. Available: https://www.zurich.com/en/knowledge/topics/cyber-and-data-risks/eighth-annual-advisen-information-security-and-cyber-risk-management-survey

[17] Deloitte, “Beneath the surface of a cyberattack. a deeper look at business impacts,” 2016. [Online]. Available: https://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.html

[18] A. Sedgewick, “Framework for improving critical infrastructure cybersecurity, version 1.0,” NIST, Tech. Rep., 2014.

[19] ISO, “ISO 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary,” *International Organization for Standardization*, 2018.

[20] ——, “ISO 27035:2011 Information technology — Security techniques — Information security incident management,” *International Organization for Standardization*, 2011.

[21] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, “Computer security incident handling guide,” *National Institute of Standards and Technology*, 2012.

[22] IBM, “Cost of a data breach report,” 2019. [Online]. Available: https://www.ibm.com/security/data-breach

[23] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. Van Eeten, M. Levi, T. Moore, and S. Savage, “Measuring the cost of cybercrime,” in *The economics of information security and privacy*. Springer, 2013, pp. 265–300.

[24] I. Agrafiotis, J. R. Nurse, M. Goldsmith, S. Creese, and D. Upton, "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate," *Journal of Cybersecurity*, vol. 4, no. 1, p. tyy006, 2018.

[25] C. M. Pearson and J. A. Clair, "Reframing crisis management," *Academy of management review*, vol. 23, no. 1, pp. 59–76, 1998.

[26] A. Boin, E. Stern, B. Sundelius, and P. 't Hart, *The politics of crisis management: Public leadership under pressure*. Cambridge University Press, 2005.

[27] BSI, "PD CEN/TS 17091:2018 Crisis management. Guidance for developing a strategic capability," 2018.

[28] S. Boeke, "National cyber crisis management: Different european approaches," *Governance*, vol. 31, no. 3, pp. 449–464, 2018.

[29] Cyber Israel, "National Cyber Concept for Crisis Preparedness and Management," Prime Minister's Office. National Cyber Directorate, Tech. Rep., 2017.

[30] P. Trimintzios, R. Holfeldt, M. Koraeus, B. Uckan, R. Gavrila, and G. Makrodimitris, "Report on cyber crisis cooperation and management," *European Union Agency for Network and Information Security*, 2014.

[31] M. J. West-Brown, D. Stikvoort, K.-P. Kossakowski, G. Killcrece, and R. Ruefle, "Handbook for computer security incident response teams (csirts)," Carneige-Mellon University, Tech. Rep., 2003.

[32] P. Johannesson and E. Perjons, *An introduction to design science*. Springer, 2014.

[33] K. E. Newcomer, H. P. Hatry, and J. S. Wholey, "Conducting semi-structured interviews," *Handbook of practical program evaluation*, vol. 492, 2015.

[34] Northwave, "Nw-cert rapid response plan," 2018, unpublished.

[35] A. Galletta, *Mastering the semi-structured interview and beyond: From research design to analysis and publication*. NYU press, 2013, vol. 18.

[36] B. L. Leech, "Asking questions: Techniques for semistructured interviews," *PS: Political science and politics*, vol. 35, no. 4, pp. 665–668, 2002.

[37] A. Bhattacherjee, "Social science research: Principles, methods, and practices," 2012.

[38] B. Herbane, “Exploring crisis management in uk small-and medium-sized enterprises,” *Journal of Contingencies and Crisis Management*, vol. 21, no. 2, pp. 82–95, 2013.

[39] Maastricht University, “Reactie universiteit maastricht op rapport fox-it,” 2020. [Online]. Available: https://www.maastrichtuniversity.nl/um-cyber-attack-symposium-\OT1\textendash-lessons-learnt

[40] SURF, “Ransomware universiteit maastricht: achter de schermen,” 2020. [Online]. Available: https://www.surf.nl/ransomware-universiteit-maastricht-achter-de-schermen

[41] T. Sterling, “University of maastricht says it paid hackers 200,000-euro ransom,” Reuters, 2020. [Online]. Available: https://www.reuters.com/article/us-cybercrime-netherlands-university/university-of-maastricht-says-it-paid-hackers-200000-euro-ransom-idUSKBN1ZZ2HH

[42] S. Gatlan, “Ransomware hits maastricht university, all systems taken down,” Bleeping Computer, 2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/ransomware-hits-maastricht-university-all-systems-taken-down/

[43] M. van den Bergh, “Universiteit maastricht kampt met ransomware-aanval,” Nederlandse Omroep Stichting, 2019. [Online]. Available: https://nos.nl/artikel/2316120-universiteit-maastricht-kampt-met-ransomware-aanval.html

[44] Maastricht University, “Updates cyberattack,” 2020. [Online]. Available: https://www.maastrichtuniversity.nl/um-cyber-attack-symposium-\OT1\textendash-lessons-learnt

[45] Proofpoint, “Ta505 distributes new sdbbot remote access trojan with get2 downloader,” 2019. [Online]. Available: https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader

[46] Avast, “What is eternalblue and why is the ms17-010 exploit still relevant?” 2020. [Online]. Available: https://www.avast.com/c-eternalblue

[47] Microsoft, “Microsoft security bulletin ms17-010 - critical,” 2017. [Online]. Available: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

[48] Top Universities, “Qs world university rankgings - 2021,” 2020. [Online]. Available: https://www.topuniversities.com/university-rankings/world-university-rankings/2021

[49] N. C. S. Center, “Ransomware - maatregelen voor het voorkomen, beperken en herstellen van een ransomware-aanval,” 2020. [Online]. Available: https://www.ncsc.nl/onderwerpen/ransomware/documenten/factsheets/2020/juni/30/factsheet-ransomware

[50] K. Lovejoy, “Ransomware: to pay or not to pay?” Ernst & Young, 2020. [Online]. Available: https://www.ey.com/en_gl/consulting/ransomware-to-pay-or-not-to-pay

[51] H. Modderkolk, “Niet betalen aan computergijzelaars klinkt goed – tot je wordt gehackt,” de Volkskrant, 2020. [Online]. Available: https://www.volkskrant.nl/nieuws-achtergrond/niet-betalen-aan-computergijzelaars-klinkt-goed-tot-je-wordt-gehackt~bf580bf6/

[52] B. Krebs, “Ransomware gangs now outing victim businesses that don’t pay up,” KrebsonSecurity, 2019. [Online]. Available: https://krebsonsecurity.com/2019/12/ransomware-gangs-now-outing-victim-businesses-that-dont-pay-up/

[53] S. Golubev, “Backing up is no panacea when blackmailers publish stolen data,” Kaspersky, 2020. [Online]. Available: https://www.kaspersky.com/blog/ransomware-data-disclosure/32410/

[54] A. Elwood, “Overcoming psychological barriers to plan invocation,” *Journal of business continuity & emergency planning*, vol. 10, no. 2, pp. 188–196, 2017.

[55] S. Elsubbaugh, R. Fildes, and M. B. Rose, “Preparation for crisis management: A proposed model and empirical evidence,” *Journal of contingencies and crisis management*, vol. 12, no. 3, pp. 112–127, 2004.

[56] P. Institute, “The impact of data breaches on reputation and share value.” [Online]. Available: https://www.centrify.com/media/4737054/ponemon_data_breach_impact_study.pdf

[57] I. L. Janis, “Groupthink,” *IEEE Engineering Management Review*, vol. 36, no. 1, p. 36, 2008.

[58] N. Vidmar, “Group composition and the risky shift,” *Journal of Experimental Social Psychology*, vol. 6, no. 2, pp. 153–166, 1970.

Appendix A

CERT Interview Guide

A.1 Background

1. What are the main reasons why companies call the CERT?
2. What would you say are the most common types of cyber attacks for which the team gets deployed?
   (a) What is the attacker's motivation?

A.2 CERT Activation

1. Let's now consider a situation where the CERT gets contacted by a company that fell victim of a cyber attack (from now on referred as "client"):
   (a) What is the purpose of primary triage?
   (b) What are the questions that are asked and what is the information that is needed to understand what is the impact of the cyber incident and whether it requires the team to dispatch?
      i. Is there any objective parameter/indicator that is particularly relevant to consider in this phase?
   (c) What is the client's typical level of understanding of the cyber incident and its impact at this stage?
   (d) What are the main challenges that arise during primary triage?
2. Considering your experience on previous cases, how frequently would you say that the CERT gets contacted too soon, at the right time or too late?
   (a) Do you think there are some common factors that could categorise the companies that call too early, at the right time and too late?

   (b) When they do, what are the most common reasons why companies call too late?

   (c) How would a more timely involvement make a difference?

A.3 CERT Deployment

Let's assume that the CERT team gets deployed to the client:

1. What is the main goal of the intake meeting at the client's site? And what are the main topics discussed?

   (a) Does the meeting also help the client better understand what the business impact is?

   (b) Who is usually involved in the meeting?

2. In your opinion, what are the main challenges that arise during the intake meeting?

3. What is important to discuss in order to get a better sense of what the business impact is and to prioritise the recovery work that has to be done?

   (a) Is there any specific documentation on the client's infrastructure that becomes relevant when deciding how to prioritise the recovery work?

   (b) Having logs that go back a considerable amount of time I would guess it is important to conduct forensic investigations. What is your experience wrt that?

4. Based on the experience with past incidents, how common is it that the client has an Incident Response Plan in place?

   (a) Why would you say it's (un)common?

   (b) What are the main disadvantages of not having one?

5. Based on the experience with past incidents, how common is it that the client has a security monitoring solution in place?

   (a) Why would you say it's (un)common?

   (b) What are the main disadvantages of not having one?

A.4 Crisis Transition

1. From your perspective, how would you differentiate a cyber incident from a cyber crisis?
   (a) Is there a specific set of triggers, indicators, thresholds that you deem relevant to mark the limit between the two?
2. Based on your experience, when the CERT gets deployed how likely is it that the incident will represent a crisis for the client organisation?
   (a) In your experience, is there a formal handover from incident to crisis?
   (b) How common is it that the client has and follows a formal Crisis Management Plan with a dedicated Crisis Management Team?
      i. In your opinion, why is it (un)common?
      ii. Considering your job as a CERT member and more broadly the activities that the CERT performs on site, does it make a difference if the client has a formal CMP or not?
      iii. What are the main disadvantages of not having one?
   (c) Do you think that cyber crises manifest as such, or rather they arise as a sequence of cyber incidents?
      i. In that case, could it be because the incident was not detected and therefore only the crisis was visible?
         A. Could this relate to why companies call too late?
      ii. Considering your experience with previous cases, would you say that monitoring could have allowed for the treatment of the incident and prevented the crisis?
3. In your opinion, when an incident is detected, is the IT alone enough to understand what is the business impact of an incident? And by extension, to understand when an incident is a potential crisis?
4. How would you say that cyber incidents are different than regular incidents?

If any specific document was mentioned throughout the interview, ask for it now and remind with a thank you email.

Appendix B

Case Study Interview Guide

B.1 Scenario

1. Before the attacker could get in, was there some other activity that suggested the company was begin targeted by cybercriminals?
   (a) How common is it to receive early signals that make the company realise they are being targeted?
2. How did the attacker get into the infrastructure?
3. Did the client have security monitoring in place?
4. Once inside, the attacker had to move through the infrastructure in order to first prepare and then deploy the ransomware.
   (a) If monitoring was in place, what activity could have been detected which would have indicated his presence?
   (b) How does this relate with experience on other cases?
5. How much time went by from the moment the attacker got into the infrastructure to when the ransomware was deployed?
   (a) The team has experience with many cases, how much time does usually go by in other cases?
6. How did the company realise that something had happened?

B.2 Crisis Management

1. During a previous conversation we discussed that it is rather common that organisations do not have crisis management plans. Did the organisation have

a CMP in this case?

(a) Was there a crisis management team in place?

i. Who was part of the CMT?

(b) In your experience what are the main disadvantages that organisations face when not having a CMP?

(c) Why is it not common for the organisations that we engage with to have a CMP?

2. Early recognition

(a) Did the company have a sense of being targeted before the attack was mounted?

(b) How common is it to have the perception that they could fall victim of a cyber attack?

i. Could this be related with the fact that many companies do not have a CMP?

(c) We previously discussed that for this case no security monitoring was in place. Is it common with other organisations as well?

i. In you opinion, what would the main reasons behind it be?

3. Sense making and meaning making

(a) The organisation manages multiple companies in 10 different countries worldwide.

i. What was the extent of the cyber attack?

ii. Was it clear from the early stages?

(b) What did the attack mean for the business operations?

(c) To make sense of what is happening, as well as to have an idea of what the impact is and prioritise work, it was highlighted as important to translate business processes to the supporting IT and vice versa. How frictionless was this activity?

i. Are there specific factors that contributed in it?

ii. How would you say is the perception of management on the reliance of the whole business on IT?

A. Has it changed over the past few years?

(d) Considering the activities that the CERT performed:

i. Having the right documentation on the infrastructure has been highlighted as an important factor for an efficient and effective resolution. How was the experience in this case?

ii. Logs that go significantly back in time have been identified as essential to conduct proper forensic investigations. Has it represented a challenge in this case?

(e) Ransomware is probably not the typical case that the board is accustomed in dealing with. How and by whom was the incident conveyed to the board and what were the challenges in that process?

4. Decision making

(a) Crises test managers to take decisions in a climate of uncertainty and time pressure. In your opinion what behaviours lead to (un)effective crisis management?

(b) Did the crisis have an effect on the morale?

i. If so, is it something that affected performance? How?

(c) At some point, a decision on whether to pay or not to pay the ransom had to be taken. What are the factors that have been considered and how was the decision matured?

i. Were there concerns related to GDPR?

ii. Was data exfiltrated in an attempt to gain more leverage?

iii. Engaging with the attacker is something that most professionals do not have experience with. What is typically the attitude of the attacker and what are the main challenges in this context?

5. Concluding remarks

(a) Did the attack also affect communication channels such as emails and telephony?

i. Did that result in a struggle in coordination?

(b) Did the incident become public?

i. If so, when and why?

(c) Considering similar cases, what are the challenges with respect to accountability and attribution of the cyber attacks?

(d) In general, do you see a tendency from to consider cybersecurity as just an IT issue?

i. Does that perception change after a cyber crisis?

ii. What do you see as effective to shift that perception?