If you can dream it, you can do it.

Walt Disney

Contents

List of Figures

1 Introduction

1.1 Introduction and thesis objectives

The WEF 2023 Global Risks Report (World Economic Forum, 2023) uses the following words to describe the critical landscape that characterises the society we are living in: *"The first years of this decade have heralded a particularly disruptive period in human history. The return to a "new normal" following the COVID-19 pandemic was quickly disrupted by the outbreak of war in Ukraine, ushering in a fresh series of crises in food and energy – triggering problems that decades of progress had sought to solve. As 2023 begins, the world is facing a set of risks that feel both wholly new and eerily familiar. We have seen a return of "older" risks – inflation, cost-of-living crises, trade wars, capital outflows from emerging markets, widespread social unrest, geopolitical confrontation and the spectre of nuclear warfare – which few of this generation's business leaders and public policy-makers have experienced. These are being amplified by comparatively new developments in the global risks landscape, including unsustainable levels of debt, a new era of low growth, low global investment and de-globalization, a decline in human development after decades of progress, rapid and unconstrained development of dual-use (civilian and military) technologies, and the growing pressure of climate change impacts and ambitions in an evershrinking window for transition to a 1.5°C world. Together, these are converging to shape a unique, uncertain*

and turbulent decade to come."

Among all the types of crises facing our society, the WEF Global Risk Perception Survey 2022-2023 (World Economic Forum, 2023) reveals that the top five having the greatest potential impact on a global scale are: "Energy supply crisis"; "Cost-of-living crisis"; "Rising inflation"; "Food supply crisis" and "Cyberattacks on critical infrastructure" [Figure 1.1]. Thus, in addition to the more traditional risks related to societal and economic domains, the ever more rapid pace of technological development and its unprecedented intertwining with the critical functioning of societies, is bringing new risks on the landscape.

Figure 1.1: *Top five crisis perceived as having the greatest potential impact on a global scale (Source: WEF Global Risk Report 2023)*

It is true that digital technologies - AI applications, edge computing, Internet of Things (IOT) devices, autonomous technologies – are creating unprecedented opportunities to improve the functioning of cities and critical infrastructures. However, the resulting convergence of digital and physical worlds, is giving rise to new challenges as well. As highlighted in the 2022 Global Risks Report (World Economic Forum, 2022) malicious activity in cyberspace is on the rise, and it is characterised by more aggressive and sophisticated attacks taking advantage of more widespread exposure.

That is why the "Widespread cybercrime and cyber insecurity" is ranked by the WEF (World Economic Forum, 2023) into the top 10 risks over the next decade. Cybercrime is perceived to be threatening the security of critical infrastructures and thus the provisioning of essential services like water, financial systems, public security, transport, energy and domestic, space-based and undersea communication, putting at risk the well-being of individuals and the functioning of societies.

If compared to other types of risks, "Widespread cybercrime and cyber insecurity" is

considered to be among the most severe both in the short and in the long term [See Figure 1.2, top right quadrant]. As stated by Larry Clinton (author of WEF Cyber Risk Handbook, and president of the Internet Security Alliance) *"the cyber equation attack methods are comparatively cheap and easy to acquire, attackers have first-mover advantage, generate high profits with a great business model. Versus the defenders protecting an inherently vulnerable system (getting more vulnerable all the time), often "out-gunned" by attackers, virtually always in reactive mode and who get virtually no help from law enforcement "* (Bonime Blanc, 2021).

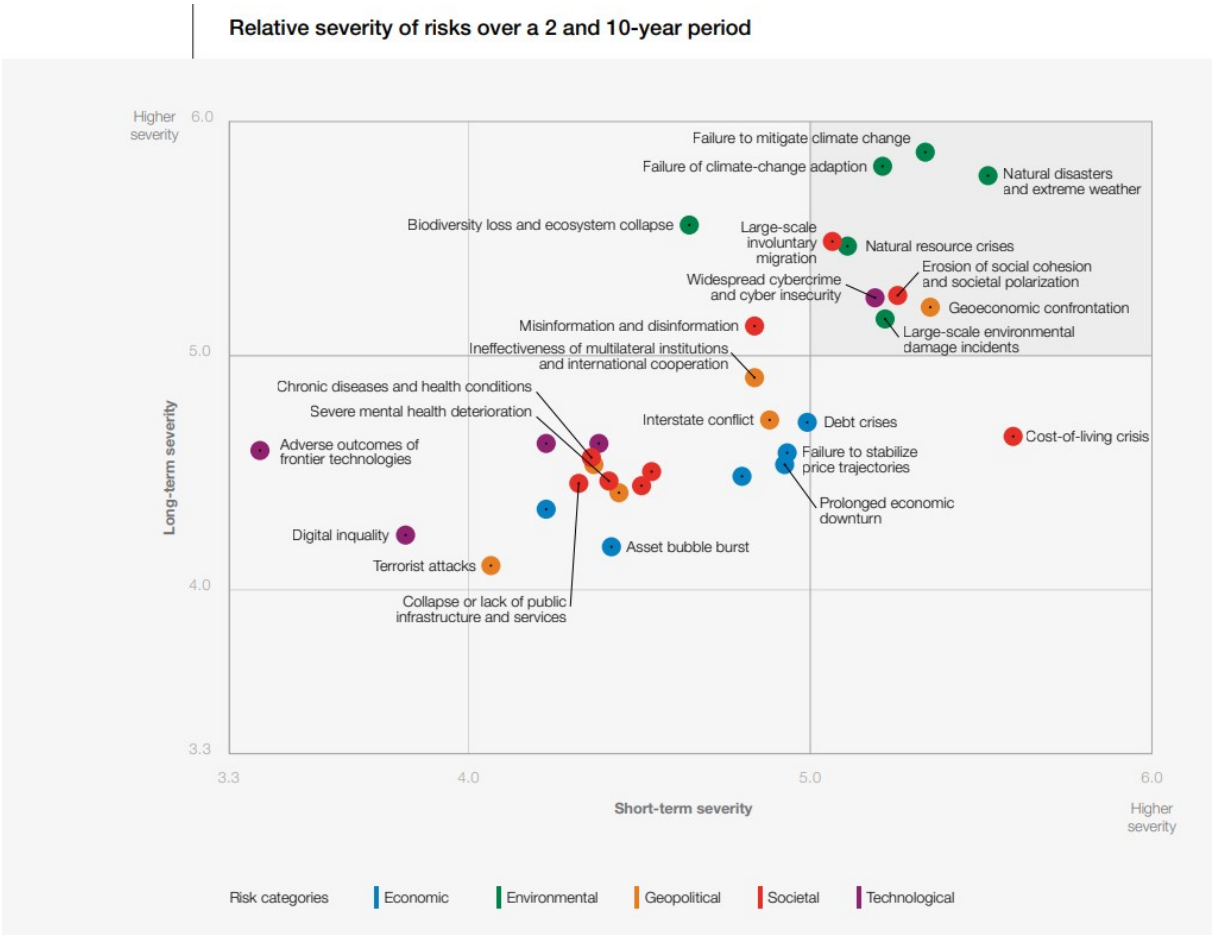


FIGURE 1.2: *Comparison of sources of risks in terms of severity and period of concern. Severity was assessed on a 1-7 Likert scale [1 Low severity, 7 High severity]. (Source: WEF Global Risk Report 2023)*

In this critical scenario, it is crucial for companies of all types to be prepared to confront any form of crisis, whether traditional or cyber-related, to survive and achieve sustainable

growth. Now more than ever, it is essential to invest resources in the adoption and development of measures, tools and core competencies for optimal crisis management. Indeed, it is widely recognized that the way in which crisis management is executed can have a significant impact on a firm's long-term success and sustainability (Pearson and Clair, 1998; Pwc and Oxford-Metrica, 2020). This impact can be so profound that companies can be categorized into two distinct groups after a crisis: "winners" who successfully recover and increase their value, and "losers" who suffer prolonged negative effects. Therefore, understanding which capabilities, processes, and tools are effective in facing crises and result in the "winner" group is imperative and vital.

Over the past years, researches have focused on investigating the factors that prove to be influential in facing a traditional organizational crisis. Among those factors, management responsiveness, leadership competencies, coordinated teams, and motivated and resilient employees have been recognised as the primary determinants of whether value is gained or lost (Bundy et al., 2017; James et al., 2011; Pwc and Oxford-Metrica, 2020; Wart and Kapucu, 2011; Williams et al., 2017; Wooten and James, 2008).

Given the increasing frequency and severity of cybercrimes on a global scale, it is rational to suggest that identifying specific factors that help companies navigating cyber-related crises (hereinafter referred to as cyber crises) would offer additional valuable insights to both researchers and practitioners. However, while cyber crises are extensively recognised as one of most severe threats facing our society, the academic literature is currently featuring very little research on this topic. A critical research gap still exists on how companies can develop optimal cyber crisis management processes and capabilities, particularly related to leadership competencies (Salviotti et al., 2023).

One of the first papers addressing this specif gap is *Understating the Role of Leadership Competencies in Cyber Crisis Management: A Case Study* (Salviotti et al., 2023) originally presented in the Proceedings of the 56th Hawaii International Conference on System Science 2023 (hereinafter referred to as the *reference paper*), which specifically focuses on determining whether the crisis leadership competencies identified by the traditional crisis management literature are actually effective in cyber crisis contexts. As the authors highlighted, *"In view of the fast evolution of cybercrimes and their detrimental consequences for organizations and society, there exists a crucial need to contribute towards augmented*

knowledge of cyber-related crises. Hence, the subject investigated is both topical and urgent".

This thesis is conceived to be an extension of the reference paper with the objective to contribute to increase knowledge in this essential field.

The results of the reference paper (that will be further discussed in the next chapter) have started to shed some light on which capabilities are effective to face cyber crises. In particular, even though a good level of alignment has been found between traditional scenarios and cyber crisis contexts, the leadership competencies needed to manage cyber crises are not necessarily equal to the ones that the academic literature suggests to successfully manage traditional crises. The authors' results and discussion has begun to scratch the surface of the topic, but further examination is still needed to provide valuable insights, models and reference frameworks in the field of cyber crisis management.

Through the analysis of different data, this thesis aims exactly at responding to that need. In particular, it uses the same approach to investigate a different case study, featuring different characteristics in terms of company type, business model and geography, namely the *Maersk global supply-chain meltdown*. The results of the analysis performed offer the possibility to confirm or disprove the findings of the reference paper, as well as the potential to reveal new elements which were not considered. This, together with the outcome of the reference paper, can be used as a valuable source of data to build a reference framework for cyber crisis leadership competencies.

1.2 Thesis structure

The thesis is organised in five chapters:

- **Chapter 2** opens with the analysis of literature regarding cybercrime and ransomware attack. It then deep dives into providing a complete perspective on the themes of crisis, crisis management and crisis leadership competencies. In doing so, the new concepts of cyber crisis and cyber crisis management are also introduced, and the current challenges and gaps identified in the relative research field are highlighted. The review is based on a selection of literature sources from established databases which are relevant to the research topic. The Chapter concludes with the description

of the reference paper and of its main findings.

- **Chapter 3** explains the methodology used to write the thesis. It first provides a general overview of the approach that was selected to investigate the new case study. It continues with a focus on the case, providing the rationales at the base of its selection and describing its main features. The Chapter finally concludes by describing the data collection procedure and detailing the first steps of the data analysis performed.
- **Chapter 4** is entirely devoted to describing the analysis of the selected case study. After providing a general overview of the cyber attack experienced, the chapter focuses on fully explaining how the cyber crisis was handled by the company's top managers and by its key employees during its various phases.
- **Chapter 5** presents the findings of the analysis and compares them to the results of the reference paper so to respond to the research question.
- The final chapter of this thesis, **Chapter 6**, contains a summary of the work presented, an appraisal of its contributions, and several suggestions for future work.

2 Literature Review

This chapter opens with a review of the literature on cybercrime and ransomware attacks providing a detailed description of the increasingly alarming threat landscape that organisations have to face. It goes on to analyse previous research that focused on understanding how to effectively manage these threats investigating the topics of crisis, crisis management and crisis leadership competencies. Given the ever rising relevance of the cyber domain, special emphasis is given to the specific concepts of cyber crisis and cyber crisis management. After having identified the current challenges and gaps in the cyber-related research field, the reference paper and its main findings are finally presented.

2.1 Cybercrime and Ransomware

"Since the turn of the twenty-first century, cybercrime has become organised and industrialised like no other crime. This maturing process has enabled would-be cybercriminals to continuously hone their skills whilst searching for the next opportunity to profit. In turn, this has created numerous cybersecurity challenges for enterprise cyber risk managers and security operations teams. Despite the continued rise of numerous new threats, it is ransomware that is now the most dangerous form of cyberattack that enterprises must be

prepared for.[. . .] In the wake of rapid technological advances in applied cryptography, the Internet and financial systems, enterprises are now more vulnerable to ransomware attacks than ever before" (Ryan, 2021). During the last decade ransomware has become one of the most disruptive types of cyberattacks causing devastating effects to organizations of all sizes worldwide (Cambridge University Center for Risk Studies and RMS, 2019; ENISA, 2022a; Ryan, 2021). The word ransomware has been increasingly dominating the headlines of cybercrimes reports which highlight the great financial losses and disruptions suffered by organizations and individuals falling victims of these attacks [See Figure 2.1] (McIntosh et al., 2021).

Year	Event
1989	The first known and documented ransomware: *AIDS Trojan* (also known as the *PC Cyborg* virus)
2006	*GPCode* and Archiveus Trojan began using more powerful asymmetric RSA encryption.
2013	*CryptoLocker*, one of the most damaging ransomware, possibly profited US$27 million
2014	*ScarePackage* ransomware was the first to target Android mobile platforms. It infected users as fake apps appearing to be Adobe Flash or other well-known antivirus, and pretended to scan user files when launched.
2015	*CryptoWall 2.0*, delivered via emails, PDF and various exploit kits, used TOR to obfuscate C&C communications, and incorporated anti-virtual-machine and anti-emulator techniques to avoid analysis via sandboxing.
2015	*Linux.Encoder* was considered the first known ransomware targeting the Linux platform.
2016	*KeRanger* was discovered as the first known ransomware targeting the MacOS platform.
2016	*PoshCoder* became the first fileless ransomware and instead used PowerShell commands to encrypt files.
2017	*WannaCry* attack propagated through the Windows EternalBlue exploits, causing an estimated USD$4billion of damage globally through loss of data and disrupted business processes.
2017	*NotPetya* was the first known ransomware to encrypt the Master File Table of the NTFS drive.
2020	*RagnarLocker* was the first known virtual-machine-based ransomware to be deployed as virtual machines and to encrypt host files via shared folders, in order to evade host-based ransomware detection.
2020	*Maze* was the first known ransomware to exfiltrate sensitive data to blackmail users into paying ransom.

Figure 2.1: *A brief history of notable ransomware episodes. (Source: McIntosh et al., 2021)*

And as Figure 2.2 shows, ransomware has become a topic of major interest also for research, mainly due to its greater existential threat to companies compared to other forms of attacks (Ryan, 2021).

However, there is still lack of agreement regarding ransomware terminology. The current definitions are mismatching and have been modified over time as ransomware has been evolving. As a reference point, the definition provided by ENISA (ENISA, 2022a) can be considered. It defines ransomware as *"a type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the asset's availability and confidentiality"*.

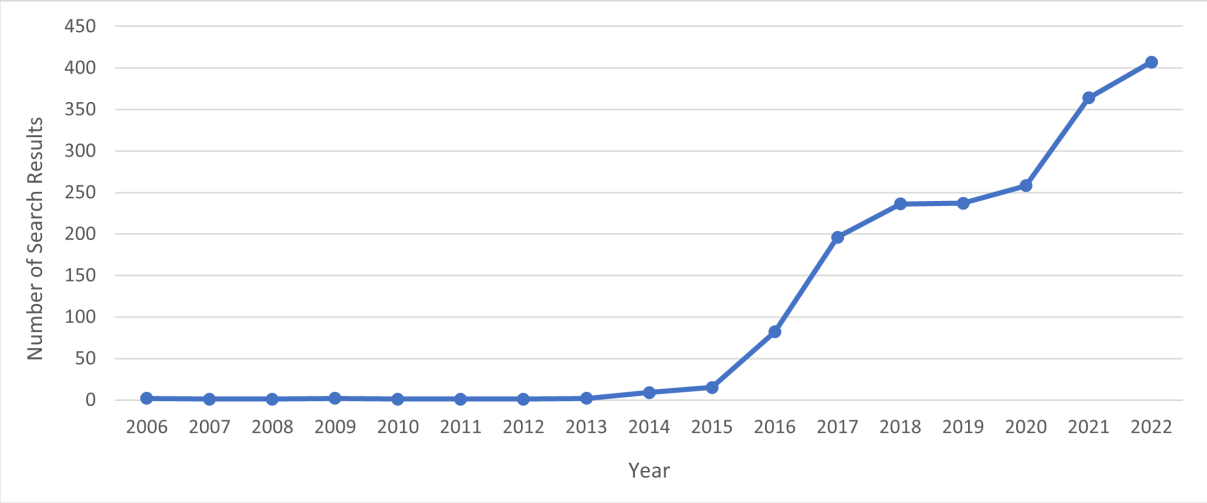


FIGURE 2.2: *Number of articles with titles containing the keywords "Ransomware" per year on Google Scholar (excluding patents and citations).*

The report highlights that ransomware is a special type of malware (which according the the NIST Glossary can be defined as a malicious software intentionally designed to harm victim's machines and systems) that features three distinctive characteristics:

- Assets, anything of value for the target victim;
- Actions, that the ransomware can execute (lock access to an asset, encrypt an asset, steal an asset, delete an asset); and
- Blackmail, which is the final step of the ransomware where the attacker coerces the victim through the use of threats demanding the payment of a ransom in return for asset availability.

As for the motivation, even though financial objective is the main one, there have been cases of ransomware threat actors demanding change in corporate policy, new software features, or asking targets to infect their social circle (ENISA, 2022a).

One additional feature of ransomware is that it is not static. In fact it has significantly evolved since the first incident was observed in 1989 leveraging new technologies and capabilities to increase its effectiveness. The market has matured, attackers have acquired innovative tools and capacities to carry out their attacks, and ransomware has become a commodity (ENISA, 2022a). Thanks to new formats, ransomware is easier to perpetrate and has many advantages to other forms of crime: it's untraceable, logistically seamless,

cheap, and it does not require huge investment in human capital (Bonime Blanc, 2021). *"When researchers examined the correlation of cyberattacks and the speed of technological adoption, they found that the ability to attack will likely outpace the ability to defend. Attackers can be hedgehogs (they only need to know one attack method, but do it well), whilst defenders must be foxes (they need to know everything, not just technical knowledge but knowledge of networking, software, law enforcement, psychology, etc.)"* (Ryan, 2021).

As for the effects, ransomware's impacts are devastating, and they go far beyond the cost of the ransom itself. The *"cost of ransom payments is relatively minor compared with the potential losses that these malware attacks can inflict from business interruption by encrypting servers, wiping critical data, and disabling vital systems"* (Cambridge University Center for Risk Studies and RMS, 2019).

Ransomware, due its transboundary nature, has the potential to hit entire supply chains, causing more widespread damage than an attack against a single individual entity. The following statistics clearly depict the breadth and growing scale of ransomware threats:

- According to the 2022 Verizon Data Breach Investigations Report (Verizon, 2022), ransomware attacks surged dramatically in 2022 and ransomware was involved in 25% of all breaches (see Figure 2.3);

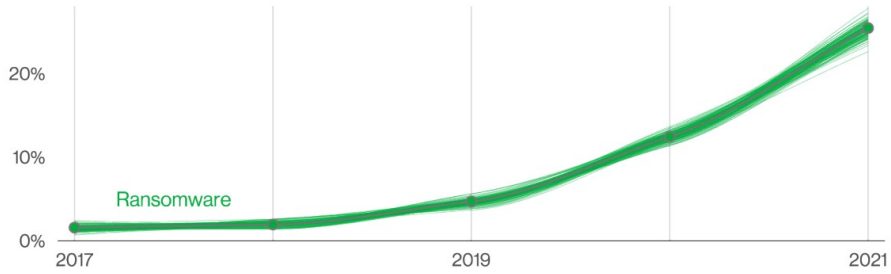


Figure 2.3: *Ransomware over time in breaches. (Source: Verizon, 2022)*

- Sophos's The State of Ransomware 2022 report (SOPHOS, 2022) highlights that ransomware affected 66% of organizations in 2021, with an increase of 78% over 2020;
- The FBI's Internet Crime Complaint Center (Federal Bureau of Investigation. Internet Crime Compliant Center, 2021) received 3,729 complaints about ransomware

attacks in 2021, accounting for financial losses of $49.2 millions;

- The Cybersecurity and Infrastructure Security Agency reported in February 2022 (CISA Cybersecurity Advisory, 2022) that 14 of the 16 U.S. critical infrastructure sectors have experienced ransomware attacks;
- In 2022 IBM (IBM, 2022) revealed that on average ransom payments amount to $812,360 and total cost of a ransomware attack costs $4.5 million. In additions, IBM highlighted that it takes an average of 49 days longer than other types of attacks for organization to identify and remediate ransomware breaches.
- CyberSecurity Venture (Braue, 2022) predicts that Ransomware will cost its victims more around $265 billion (USD) annually by 2031, with a new attack happening (on a consumer or business) every 2 seconds as ransomware perpetrators progressively refine their malware payloads and related extortion activities [See figure 2.4].

Year	Global Ransomware Damage Costs
2015	$325 Million
2017	$5 Billion
2021	$20 Billion
2024	$42 Billion
2026	$71.5 Billion
2028	$157 Billion
2031	$265 Billion

FIGURE 2.4: *Expected global ransomware costs over the next years. Source: Cybersecurity Ventures (**Braue**, **2022**)*

This alarming threat landscape makes it clear that ignoring the cyber problem could become the costliest (potentially existential) crisis for companies, impacting people, assets and profits (Salviotti et al., 2023). Evidently, the industry must take steps to confront this unique, constantly evolving risk.

2.2 Crisis and Crisis Management

> *It is no longer a question of if a crisis will occur; it is rather, a question of when, what type and how to be better prepared to up against it.*
>
> (Benali and Ghomari, 2016)

Understanding the terminology used within the field of crisis management is crucial because how a subject is defined indicates how it is approached (ENISA, 2022b; Wart and Kapucu, 2011). Perception and terminology related to crisis and crisis management indeed have greatly evolved over time resulting in a plethora of different perspectives and concepts used by organizations, nations and academia. Many books and academic papers have been written about this topics, but conceptions vary considerably and hardly a unique and accepted definition of either crisis or crisis management can be found (Coombs, 2022; Perry and Quarantelli, 2005; Rosenthal, 2003; Rosenthal et al., 1989).

This is mainly because of the interdisciplinary nature of crisis that over time has led academics to choose to focus their research on just one of the multiple dimensions from which crisis can be studied, namely the psychological, the social-political or the technological-structural dimensions (Pearson and Clair, 1998). Only few scholars have explicitly chosen to adopt a multidisciplinary approach integrating the different perspectives. The outcome of this extremely variegated approach is a *"tower of babel"* effect, leading to *"many different disciplinary voices, talking in different languages to different issues and audiences"* (Shrivastava, 1993).

To solve this issue, the re-framing work performed by Person and Clair (Pearson and Clair, 1998) is brilliant. By starting from the different perspectives of crisis and crisis management they succeeded in deriving a unique and comprehensive definition which integrates all the different viewpoints in the field. The authors provide the following definitions:

- **Crisis** *"is a low-probability, high impact situation that is perceived by critical stakeholders to threaten the viability of the organization and that is subjectively experienced by these individuals as personally and socially threatening. Ambiguity of cause, effect an means of resolutions of the organizational crisis will lead too disillusionment or*

loss of psychic and shared meaning, as well as to the shattering of commonly held beliefs and values and individuals' basic assumptions. During the crisis, decision making is pressed by perceived time constraints and coloured by cognitive limitations";

- **Crisis management** *"involves minimizing potential risk before a triggering event. In response to a triggering event, effective crisis management involves improvising and interacting by key stakeholders so that individuals and collective sense making, shared meaning, and roles are reconstructed. Following a triggering event, effective crisis management entails individual and organizational readjustment of the basic assumptions, as well as behavioural and emotional responses aimed at recovery and readjustment ".*

According to those comprehensive definitions, the term *crisis* is used to refer to an event that shows some peculiar characteristics (Coombs, 2022; ENISA, 2022b; Wart and Kapucu, 2011):

- It threatens fundamental values and functions of the organization;
- It is unexpected and characterised by highly uncertain circumstances;
- It features time pressure, and decision making has to be performed in restricted amount of time;
- It cannot be handled with ordinary resources and capabilities.

In light of this, *crisis management* captures the process that directs organizations' activities for the purpose of effectively manage a highly salient, unexpected and disruptive event to restore normal operations and values as quickly as possible with minimum impact on either the business or the users (ENISA, 2022b; Mitroff and Alpaslan, 2003; Mitroff and Pearson, 1993; Paraskevas, 2006; Sahin et al., 2015).

Scholars have deeply investigated how firms respond to crises as it is widely recognised that the ability to manage unpredictable and abnormal events (financial crisis, terrors, industrial accidents, natural emergencies) is essential for their sustainable performance and survival (Duchek, 2020; Hu et al., 2022; Potocan and Nedelko, 2021; van der Vegt et al., 2015; Williams et al., 2017). The way crisis management is performed can really make a difference in the long term (Pearson and Clair, 1998; Pwc and Oxford-Metrica, 2020) to the extent that firms emerging from crises can be divided into clearly distinct groups: those that succeed to recover and ultimately go on to increase value, "winners",

and those that suffer long-term losses, "losers".

The mishandling of a crisis indeed is proved to have negative and undesirable long-term consequences for the organization and its stakeholders (Garcia, 2006; Pearson and Clair, 1998). Evidence in this regard is plentiful, visible and measurable, whether in loss of life, depletion of resources, contamination of the environment, or damage to organizational reputation. Crisis damage extends beyond financial loss, however, to include injuries or deaths to stakeholders, structural or property damage (on and off site), ruining of a reputation, damage to a brand, and environmental issues (Loewendick, 1993). The financial costs of some crises have exceeded one billion dollars; the devastation brought by these crises has included loss of hundreds of human lives as well as immeasurable damage to future generations and to the environment (Pearson and Mitroff, 1993).

But organizations may also experience beneficial effects if crisis management is effective and successful. In a 1959 speech, John F. Kennedy famously said *"When written in Chinese, the word 'crisis' is composed of two characters—one represents danger and one represents opportunity"* (Papers of John F. Kennedy, 1959). Although today it is widely recognized that this is not the correct interpretation of the Chinese characters (Mair, 2009), his intuition was correct. He suggested that out of crises can emerge new and incredible opportunities, particularly when traditional approaches and paradigms are questioned and challenged. During a crisis, incentives and motivations change significantly, and if effectively managed, that can potentially lead to new cooperative behaviours and even to the creation of new systems or structures (Langan-Riekhof et al., 2017).

Behavioural responses to the crisis may result in the restoration of individuals' sense of self-integrity and the social order, as well as in the creation of positive organizational change and enhanced organizational effectiveness (Bartunek, 1984; Pearson and Clair, 1998). Moreover, a fast, positive, and effective response to the crisis can not only allow to control the situation so to minimize negative impacts in the short term, but it also leads to increased market share, improved employee relations, and better public image about the organization in the long term.

This distinction between winners and losers is clear when looking at Figure 5 (Pwc and Oxford-Metrica, 2020). As expected, all crises have immediate negative effects on value. However, companies failing to manage a crisis (red line in Figure 2.5) experience more

than 10% decrease in stock price after the first week and 15% decrease below pre-crisis prices after 250 trading-days. On the contrary those able to successfully face the adverse event (blue line in Figure 2.5), lose just less than 5% in stock price after the first week, and in the long term they feature a quick stock recovery eventually increasing their price relative to the pre-crisis one.

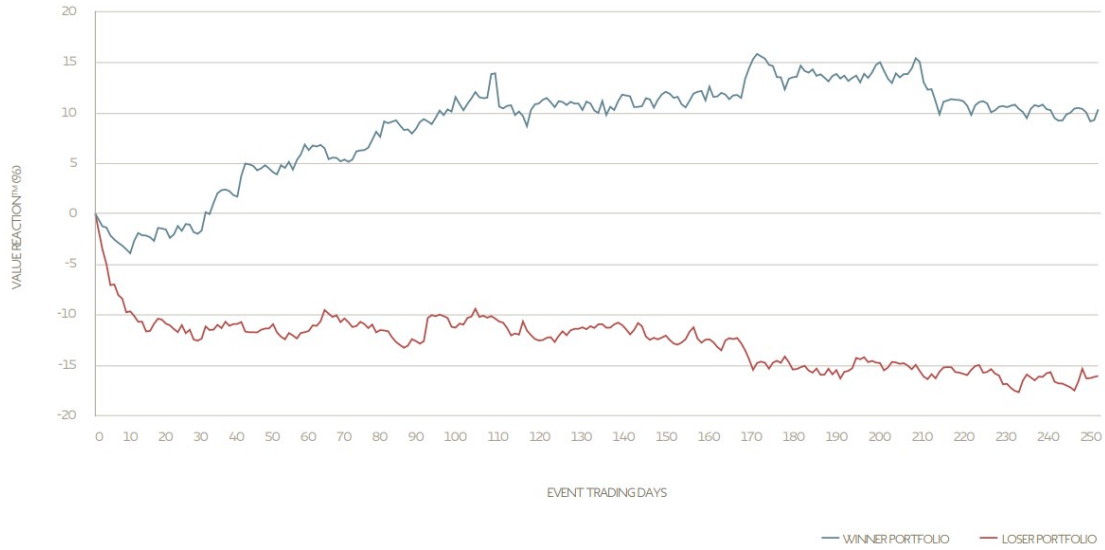


FIGURE 2.5: *The impact of crisis on share prices. (Source: Pwc and Oxford-Metrica, 2020).*

In light of the above evidence, it is therefore essential for companies to ensure they develop and sustain capabilities, processes and tools to effectively face crisis and be in the "winner" group. Several factors determine whether a firm emerges with a positive or negative impact after a crisis. However, researches agree that management responsiveness and leadership competencies are the key determinant of whether value is created or lost, since top management is directly responsible to coordinate resources and facilitate communication (Bundy et al., 2017; James et al., 2011; Pwc and Oxford-Metrica, 2020; Wart and Kapucu, 2011; Williams et al., 2017; Wooten and James, 2008). In fact, the market's evaluation of the effectiveness of management's response to a crisis, greatly contributes to determine whether shareholder value is lost, regained or even enhanced.

Multiple approaches have been developed to study crisis management with the objective to build models to help companies draft a response plan and strategy specific to face crisis.

Coombs (Coombs, 2022), has performed a review of the different frameworks and he has derived the 3 most influential ones [see Figure 2.6]:

- **Fink's approach** (Fink, 1986) which is one of the first approaches framing crisis as an extended event that does not just happen, but that evolves. He divides crisis in four phases: (1) prodromal: clues and hints of an impending crisis begin to emerge; (2) crisis breakout: a triggering event occurs along with the resulting damages; (3) chronic: the repercussions of the crisis persist as cleanup efforts continue; (4) resolution: the crisis finally reaches a termination.
- **Mitroff's model** (Mitroff, 1994) which divides crisis management into five phases: (1) signal detection: new crisis warning signs should be identified and actions should be taken to prevent it; (2) probing and prevention: organization members search known crisis risk factors trying to minimize their potential impact; (3) damage containment: a crisis hits and organization members try to contain the damage and avoid it spreads into uncontaminated parts of the organization or its environment; (4) recovery: organization members work to return to normal business operations as soon as possible; and (5) learning: organization members review and critique their crisis management efforts.
- **The three-stage model** used by a variety of crisis management experts [for example (Coombs and Holladay, 2001; Guth, 1995; Mitchell, 1986)] and that divides the crisis management into three macro-stages: precrisis (encompassing all of the aspects of crisis preparation); crisis (includes the actions taken to cope with the trigger event) and postcrisis (reflects the period after the crisis is considered to be over or resolved).

Fink	Mitroff	Three-Stage
1. Prodromal	1. Signal detection 2. Probing and prevention	1. Precrisis
2. Crisis breakout 3. Chronic	3. Damage containment 4. Recovery	2. Crisis
4. Resolution	5. Learning	3. Postcrisis

Figure 2.6: *Comparison of Staged approaches to crisis management. (Source: Coombs, 2022).*

Coombs also highlights how both Fink's and Mitroff's models naturally fit into the more general three-stage approach [See Figure 2.6].

The work performed by Coombs (Coombs, 2022) is egregious and offers a comprehensive guide full of best practices and recommendations derived from the analysis of previous work, which is extremely useful for crisis managers to optimally face each step of the crisis.

2.3 The new concepts of Cyber Crisis and Cyber Crisis Management

The vigorous growth of the cyber domain opens a new chapter in the book of crisis. It is a significant element that has to be integrated since it *"constitutes a new hotbed of potential crises"* (Prevezianou, 2020). It is undeniable that the societal developments of the last decade have made ICT systems an essential part of our daily lives fundamentally changing how we live and work, interact with one another and participate in the society (ENISA, 2022b; Prevezianou, 2020).

The opportunities brought by the advent of the cyber space are unprecedented, but this is also true for its related challenges and risks. The increasing reliance of the society on the functioning of digital technologies and cyberspace is resulting in vulnerabilities having greater potential negative consequences on our society (Bonime Blanc, 2021; ENISA, 2022b; Prevezianou, 2020). This has opened a new research field in the crisis literature, specifically aimed at analysing cyber crisis and cyber crisis management. Many scholars have tried to conduct a conceptual analysis of the terminology and questioned whether the vast knowledge gained in the traditional crisis domain remains still relevant in the cyber crisis management field [some example: (Backman, 2020; ENISA, 2022b; Golandsky, 2016; Prevezianou, 2020)].

However, despite its rising relevance, cyber crisis still remains a largely unexplored phenomenon. There is a general lack of clarity relative to its definition and further investigation is needed (ENISA, 2022b; Prevezianou, 2020). The European Union Agency for Cybersecurity, ENISA, defines cyber crisis as *"an abnormal and unstable situation that threatens an organization's strategic objectives, reputation or viability. An event that strikes at the heart of the organization"* (ENISA, 2022b).

Recently academic consensus has been achieved on framing cyber crisis as a transboundary

crisis, according to the concept theorised by Boin (Boin and M. Ekengren, 2014): *"[transboundary crisis] thrives on fragmentation and variety. Its complexity defines governmental efforts to understand its causes, pathways and potential remedies. The modern crisis does not confine itself to a particular policy area (say health or energy); it jumps from one field to the other, unearthing issues and recombining them into unforeseen mega-threats. The modern crisis is not boxed in by set dates that mark a clear beginning and end; it is an embedded vulnerability that emerges, fades, mutates and strikes again"*. Transboundary crisis thus tend to lead to a rapid escalation of the impacts, creating spill over effects that proliferate across multiple jurisdictions and borders, affect different policy areas, sectors, states and critical infrastructures (Ansell and Keller, 2010). In this scenario, a well-structured and efficiently executed cyber crisis management plan can be the differentiator between cyber attack survival and extinction (Golandsky, 2016).

However, while huge research has been done to improve firms' ability to manage traditional crises, there is still a gap in the field of cyber crisis management which *"calls for academic exploration of this terra incognita"* (Prevezianou, 2020).

2.4 Leadership Competencies and Crisis Management

The relevance of leadership competencies in crisis management has been widely highlighted by many scholars (Coombs, 2022; Salviotti et al., 2023; Wart and Kapucu, 2011). The role of organizational leaders and the impact of their decisions and actions are magnified during times of crisis, and thus their attitude, and the way they act and make decisions, can have a major impact on the effectiveness of the crisis management (Coombs, 2022; Fink et al., 1971; Wart and Kapucu, 2011). According to James and Wooten (James and Wooten, 2005) *"is often the (mis)handling of crises, not the crisis itself, that can have the most consequences – positive and negative – for a firm. What differentiates those firms that thrive during and following a crisis from those that do not is the leadership displayed throughout the process"*. Scholars agree that to successfully lead a company through the various stages of the crisis and to guarantee full recovery, a complex and broad set of leadership competencies is needed (Bolman and Deal, 1997; Burnett, 2002; James and Wooten, 2005).

Given the importance of this subject, James and Wooten (Wooten and James, 2008) have developed a leadership competencies framework for crisis management. Using the Mitroff's crisis model (Mitroff, 1994), they identified the leadership competencies that are effective and desirable for each of the five stages of the crisis, which are summarised in the Figure 2.7.

This framework is very useful for companies as it can be used as a tool to assess their current level of crisis-leadership preparedness, develop specific learning and training programs to improve in identified areas, and ensure the adoption of all the competencies needed to successfully lead a crisis. However, this framework is general and not specific to cyber crisis. Thus, the question of whether it is still relevant to effectively lead cyber crisis naturally emerges. The new transboundary nature of crisis indeed increases the complexity of the already composite response settings and its *"tendency to cross borders will involve different dynamics and result in different crisis management challenges as well requirements in terms of governance structures, crisis management capacities and cooperation in comparison to ordinary crisis"* (Backman, 2020). As a result, a cyber crisis may also require additional leadership competencies, with a different timing, and with different priorities (Salviotti et al., 2023).

Despite the criticality of the topic, there is very little in the current literature addressing this research area.

Crisis phase	Leadership Competencies	Description
Signal Detection	Sense making	Ability to make sense of apparently unrelated events to gain a complete understanding of what is happening
	Perspective taking	Ability to take the perspective of all different stakeholders involved to act in their best interests
Prevention and preparation	Issue selling	Ability to persuade top management to set or change the strategic direction of a firm. It is essential to guarantee optimal emphasis is placed on crisis planning and preparation
	Organizational agility	Ability to have a thorough knowledge of all the aspects of the business. It is necessary to guarantee a comprehensive crisis plan that works across different functions and departments
	Creativity	Ability to come up with new and innovative ideas, processes, or procedures. In crisis management it allows to find new vulnerabilities of the firm
Containment and damage control	Decision making under pressure	Ability to make sound and rapid decision under pressure, with limited information and with emotional and cognitive constraints
	Communicating effectively	Ability to connect with key stakeholders to provide or solicit necessary information and instructions guaranteeing transparency, consistency, and confidence
	Risk taking	Ability to accept a certain degree of risk to avoid excessive narrowing of possible response options, and ensuring firm's ability to strategize novel ways for overcoming the crisis
Business recovery	Promoting organizational resiliency	Capacity to absorb strains and improve the functioning of the organization in the face of adversity
	Acting with integrity	Ability to engage in ethical decision making and consistent behaviours to maintain or re-gain stakeholders' trust
Learning and reflection	Learning orientation	Ability to adopt a learning orientation and use past experience to continue developing new routines and operations to improve the way the company operates

Figure 2.7: *James & Wooten (2008) crisis leadership competencies model.*

2.5 Summary and main results of the Reference Paper

One of the first papers starting to fill the gap in cyber crisis management field is *Understanding the Role of Leadership Competencies in Cyber Crisis Management: A Case Study*, presented in the 56th HICCS, 2023, which is aimed at understanding how and to what extent leadership competencies contribute to mitigate the negative impacts of a cybersecurity crisis (Salviotti et al., 2023).

The particular research question chosen by the authors was: *how do leadership competencies contribute to mitigate the negative impacts of a cybersecurity crisis?*

To answer the question, they focused on the application of the crisis management leadership competencies model developed by Wooten & James (2008) described in the previous section, to the analysis of the cyber crisis case of Norsk Hydro, a Norwegian company that in 2019 fell victim of a devastating ransomware attack. Norsk Hydro case was considered to be appropriate by the authors, not only because widely recognised as one of the "gold standard" of the cybersecurity industry, but also because of its honesty, transparency and enlarged base of available information, essential features to perform an effective analysis.

Using the narrative inquiry technique, the authors performed a deep qualitative analysis of the data collected to gain a detailed understanding of how the cyber crisis was managed. By the application of the coding process (see subsection 3.5.2), ten major Third Order Themes were identified and were eventually assigned to the corresponding phase of the crisis (pre-crisis stage, during-crisis stage, post-crisis stage) in which they were found to be relevant. Finally, the results were interpreted through the lens of the Wooten & James (2008) Model [See Figure 2.8].

This methodology allowed the authors to have a comprehensive picture of the organizational competencies and activities that shaped the way Norsk Hydro responded to the crisis [See table on the right of Figure 2.8]. Matching them to the capabilities modelled by the traditional crisis management framework [See table on the left of Figure 2.8] enabled the authors to derive conclusions on whether the traditional leadership capabilities are still relevant and effective to face cyber crisis.

The paper interestingly confirms that some of the leadership competencies included in the

traditional model are equally important to properly handle cyber crisis (the most relevant being *issue-selling*, *communication*, and *the ability to make decision under uncertainty*). However, differently from what the traditional model prescribes, the authors found that *creativity*, *acting with integrity* and *organizational agility* are competencies which become particularly relevant to face a cyber crisis and should be adopted during all the crisis stages. Finally, one additional competence, which was not included in the traditional model, resulted to be critical for a successful restoration from the crisis, namely the *ability to implement the learnings* from the crisis. This competence is considered by the authors as one of the main pillars to enhance the cybersecurity posture of the organization, eventually contributing to the creation a more resilient cybersecurity culture.

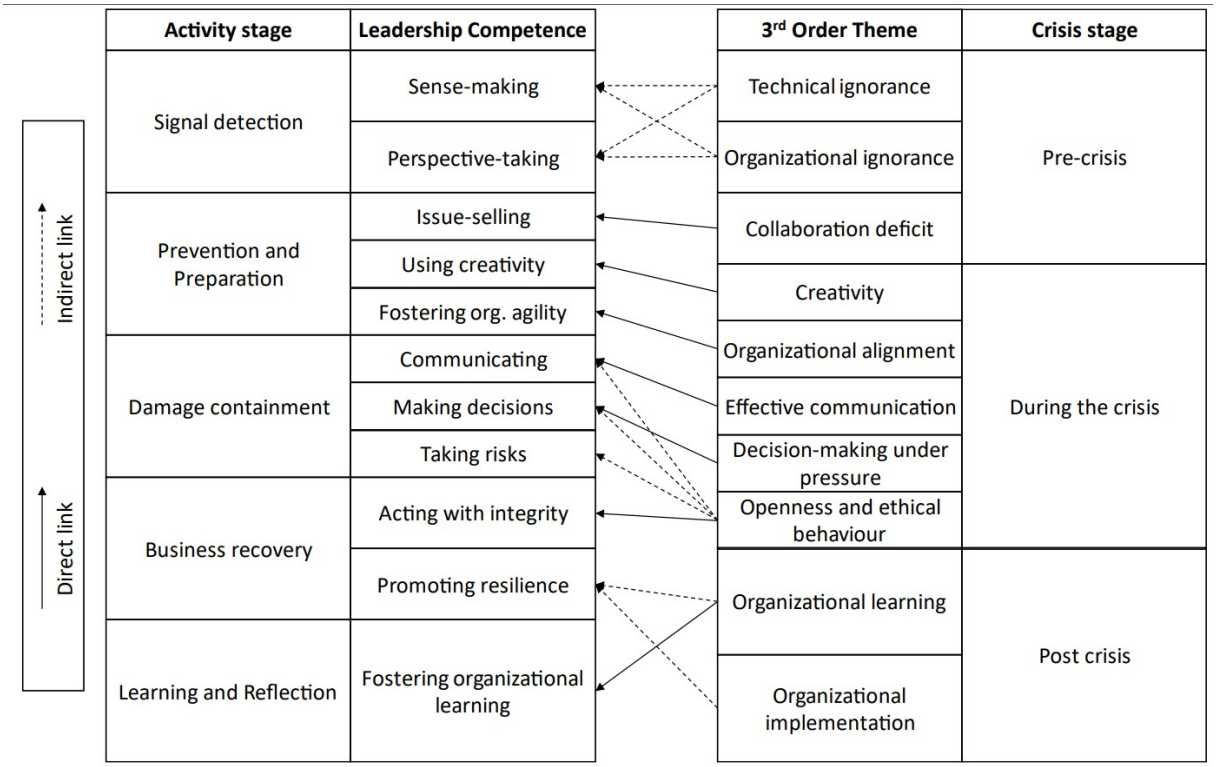


Figure 2.8: *James and Wooten Model applied to the Norsk Hydro case. (Source: Salviotti et al., 2023)*

These results evidently provide initial insights into understanding which are the relevant capabilities required to successfully handle cyber crisis situations. However this is just a starting point, and further investigation is required to develop useful models and frameworks for cyber crisis management.

The purpose of this thesis is to expand on the reference paper and advance knowledge in this critical field. By analyzing a new case study this research aims to verify or challenge the reference paper's findings and potentially uncover previously unconsidered elements.

2.6 Literature Review Summary Table

Figure 2.9 and Figure 2.10 organize and summarize the main findings of the literature review performed in this Chapter.

Topic	Main Findings	References
Cybercrime and Ransomware	• In recent years, cybercrime has undergone a rapid evolution by leveraging technological advancements, and it has become more industrialised and organised. As technology continues to advance, cybercrime is likely to become even more complex and challenging to detect and prevent. • The increasing adoption of digital technology has led to a greater vulnerability surface for companies, institutions, critical infrastructures, and societies, making them more susceptible to cyber threats. • Among the various types of cyber attacks, ransomware poses a greater existential threat to companies, and is currently the most prevalent type of malware. • Because ransomware is constantly evolving and changing, countering it has become increasingly challenging. • Ransomware costs go far beyond financial losses to the company affected, causing widespread disruption to entire supply chains and causing destabilizing effects to entire societies. • Despite its significance, there remains a research gap in the field, and there is a lack of consensus regarding the terminology used to describe ransomware and related topics.	Bonime Blanc (2021); Braue (2022); Cambridge University Center for Risk Studies and RMS (2019); CISA Cybersecurity Advisory (2022); ENISA (2022a); Federal Bureau of Investigation. Internet Crime Compliant Center (2021); IBM (2022); McIntosh et al. (2021); Ryan (2021); Salviotti et al. (2023); SOPHOS (2022); Verizon (2022); World Economic Forum (2023);
Crisis and Crisis Management	• Over time, the perception and terminology related to crisis and crisis management have evolved significantly due to their interdisciplinary nature. A unique and comprehensive definition of both terms has been derived by integrating the various different viewpoints. • The term crisis is used to refer to an event that poses a threat to fundamental values, is unexpected, has time pressure, and cannot be handled with ordinary resources. • Crisis management is the process that directs an organization's activities to effectively manage a crisis, minimizing its impacts. • The ability to manage a crisis is recognised as essential for a company's long-term growth and sustainability. • Mishandling a crisis can have negative long-term consequences for the organization, while effective crisis management can lead to beneficial long-term effects and increased value for the company. • The main factors that influence the effectiveness of crisis management are found to be management responsiveness and leadership competencies. • Established and recognized models are available to help companies building those capabilities.	Bartunek (1984); Benali and Ghomari (2016); Bundy et al. (2017); Coombs and Holladay (2001); Coombs (2022); Duchek (2020); ENISA (2022b); Fink (1986); Garcia (2006); Guth (1995); Hu et al. (2022); James et al. (2011); Langan-Riekhof et al. (2017); Loewendick (1993); Mitchell (1986); Mitroff and Alpaslan (2003); Mitroff (1994); Mitroff and Pearson (1993); Paraskevas (2006); Pearson and Clair (1998); Pearson and Mitroff (1993); Perry and Quarantelli (2005); Potocan and Nedelko (2021); Pwc and Oxford-Metrica (2020); Rosenthal (2003); Rosenthal et al. (1989); Sahin et al. (2015); Shrivastava (1993); van der Vegt et al. (2015); Wart and Kapucu (2011); Williams et al. (2017); Wooten and James (2008)

Figure 2.9: *Literature Review Summary Table - Part 1*

Topic	Main Findings	References
Cyber Crisis and Cyber Crisis Management	• A new research field has emerged in the crisis literature, specifically focused on analysing cyber crises and cyber crisis management. • Despite its increasing relevance, cyber crises still remain largely unexplored phenomena. • Cyber crises are characterized as transboundary crises, featuring rapid escalation of impacts that affect multiple entities and jurisdictions. • In contrast to traditional crises, there is a significant research gap in the field of cyber crisis management. Understanding whether the extensive knowledge gained in the traditional crisis domain remains relevant in the cyber crisis management field is essential, but it is still an open question.	Ansell and Keller (2010); Backman (2020); Boin and M. Ekengren (2014); Bonime Blanc (2021); ENISA (2022b); Golandsky (2016); Prevezianou (2020)
Leadership Competences and Crisis Management	• Scholars agree that successfully leading a company through various stages of a crisis and ensuring full recovery requires a complex and broad set of leadership competencies. • The James & Wooten model (2008) is a widely recognized framework that helps companies identify and adopt the necessary leadership competencies to effectively manage a crisis. • The question of whether this model is still relevant in effectively leading cyber crises remains relevant and still features significant research gap.	Backman (2020); Bolman and Deal (1997); Burnett (2002); Coombs (2022); Fink et al. (1971); James and Wooten (2005); Mitroff (1994); Salviotti et al. (2023); Wart and Kapucu (2011); Wooten and James (2008)
The Reference Paper	• *Understanding the Role of Leadership Competencies in Cyber Crisis Management: A Case Study* is one of the first papers to explore the impact of leadership competences in cyber crisis management. • The Norsk Hydro case was analysed through the lenses of the James & Wooten (2008) model. • The investigation was aimed at understanding whether traditional leadership capabilities are still relevant and effective when facing cyber crises. • The results of the analysis highlight that while some competences remain relevant, some new skills emerge as the key drivers for successfully facing cyber crises.	Salviotti et al. (2023)

FIGURE 2.10: *Literature Review Summary Table - Part 2*

3 Methodology

The entire chapter is dedicated to outlining the methodology employed for analyzing the new case study. As previously outlined in the Introduction chapter, the same investigative approach used in the reference paper for the analysis of Norsk Hydro case was chosen. This was essential to achieve the thesis objective.

To extend the results of the reference paper, it was indeed imperative that the outcomes and the insights derived from the analysis of the new case study were comparable with the ones derived by the authors. This eventually contributed to guarantee quality and consistency of the final results.

Thus, this thesis employed the same tools and frameworks carefully selected by the said authors, details of which will be presented in subsequent sections.

3.1 Narrative Inquiry approach

> *Not everything that counts can be counted, and not everything that can be counted counts.*
>
> Albert Einstein

The research approach chosen by the authors of the reference paper was the Narrative Inquiry as it was considered to be the most suitable methodology to answer the research question. To effectively assess the role that leadership competencies played during the management of the Norsk Hydro ransomware attack, it was essential to capture and analyse the experiences and feelings of those people that played major roles during the cyber crisis. The possibility to look at the events from the lens of those who actually experienced it, was considered by the authors to be the most effective way to understand how and to what extent leadership competencies contributed to respond to the crisis (Salviotti et al., 2023).

Narrative Inquiry is an approach to research that seeks to understand and analyze the stories people tell about their experiences. In this approach, stories themselves become row data and the focus is on the narrative itself, as well as the context and meaning behind it. One of the primary benefits of narrative inquiry is its ability to capture the complexity and diversity of human experience. Researchers often seek to categorize and quantify data, but this approach can miss the nuance and richness of individual stories. Narrative Inquiry on the contrary allows researchers to explore the unique experiences of individuals. By focusing on the stories people tell, they can gain insight into the ways in which individuals perceive and make meaning of their experiences. This approach can help to provide a more detailed and holistic understanding of the phenomenon being studied.

Furthermore, narrative inquiry allows to emphasize the role of context by recognizing that stories are shaped by the social and cultural frameworks in which they are told. This approach encourages researchers to consider the broader social, cultural, and historical factors that shape individuals' experiences and perspectives, gaining a deeper understanding of the factors that influence their actions and choices (Butina, 2015; Clandinin and Connelly, 2000; Polkinghorne, 1995; Riessman, 2008). The types of data used for narrative inquiry approach are diverse and typically include personal narratives, autobiographies

and memories, field notes and observations, artifacts and secondary sources (Butina, 2015).

Evidently, this approach results to be suitable for organizational research, particularly in the context of studying leadership and organizational change. Leadership competencies can indeed be deeply understood through the stories and experiences of leaders, which can be analysed and explored using Narrative Inquiry (Flick, 2018; Gabriel, 2000).

In this thesis, Narrative Inquiry approach was used to study the selected case in order to derive insights on how leaders acted during the crisis, the leadership competencies they demonstrated, the challenges they faced, and the strategies they used to overcome those challenges.

3.2 Choice of the case study: Maersk global supply-chain meltdown

A crucial step in the research process was the selection of the case study that best fitted the research question so to provide valuable insights to the phenomenon being studied. In particular, when choosing the case study, multiple cases involving organizations being targeted by a ransomware attack were considered and compared in terms of appropriateness and relevance.

The following criteria were used in the comparison (Eisenhardt, 1989; Salviotti et al., 2023; Stake, 1995; Yin, 2014):

- **Relevance**: case's potentiality to provide insight into the phenomenon being studied, and to test and extend the insights provided by the reference paper
- **Information richness**: ability to provide a detailed and comprehensive description of the phenomenon being studied. This criterion was important because it was at the base of the ability to gain a deep understanding of the case so to identify key patterns and themes.
- **Variability**: diversity in terms of the context, settings, and stakeholders involved. This criterion was particularly important to guarantee the selection of a case featuring different characteristics relative to the one chosen in the reference paper.
- **Time-frame**: the attack had to be prior to 2020 to enable the study of the post-crisis

activities, one of the fundamental steps of the crisis management process.

- **Stakeholders involved**: the case had to feature the active participation of the management during the crisis activity so to be able to capture their experiences, as required to fully answer the research question.

Based on these criteria, the *Maerks Global Supply-Chain Meltdown* Case Study was selected. Figure 3.1 summarises the reasons that led to the selection of this specific case.

Criterion	Maersk Case
Relevance	Maersk was one of the most high-profile victims of the NotPetya cyberattack, with the company experiencing significant disruption to its operations and infrastructures. Maersk response to the cyber crisis is widely regarded as effective and efficient given the scale of the impact, and therefore it perfectly lends itself to conducting the analysis to assess how the crisis was managed and which leadership competences played a key role in the different phases of the response.
Information Richness	Maersk case presents a large amount of public information and testimonies released by the top managers and key employees which were directly involved during the various phases of the crisis. Recordings of panel discussions, interviews, podcasts, articles, blogs, and papers are publicly available, and represent a valuable and rich source of data to conduct the analysis.
Variability	Maersk case offers a different scenario compared to the one presented by Norsk Hydro case which was selected by the authors of the reference paper. The two companies operate in different sectors and geographies, which translates in different requirements in terms of business models, value chains, stakeholders involved, policies and procedures. Furthermore, they were hit by two different ransomware attacks in different period of times. This variability constitutes an essential element to broaden the scope of the investigation.
Time-frame	The cyber crisis was experienced on June 27, 2017, so prior to 2020. This allows to also evaluate the post-crisis activities performed by the company in the years following the attack.
Stakeholders involved	In Maersk case, many different stakeholders where involved, including both top managers and more operative figures which were involved on different fronts during the crisis and played different roles in the response activities. Thus, their testimonies provide a complete perspective of what happened, guaranteeing the validity of the analysis.

Figure 3.1: *Reasons for the selection of the Maersk case*

The next paragraph will be devoted to give an overview of the company's story and to

provide a detailed description of the NotPetya attack, with a particular focus to the historical context in which it happened.

3.3 Maersk, a brief summary of the story

A.P. Moller-Maersk, commonly known as Maersk, (Maersk Company Website) is a global integrated logistics company that provides end-to-end supply chain solutions to its customers. The company operates in a wide range of sectors including ocean shipping, port services, logistics and supply chain management.

Maersk was founded in 1904 by Arnold Peter Moller in Copenhagen, Denmark, when he purchased a used steamship operating out of the Danish port of Svendborg. The golden circumstances of trade and shipping which emerged during the First World War helped to establish A.P. Moller - Maersk as a leading shipping company in Denmark. After that, the company quickly expanded its operations and began to serve other regions, such as Asia and North America.

During the Second World War, when German forces occupied Denmark on 9 April 1940, the Maersk fleet was made up of 46 ships, 36 of which were outside of Danish waters and ultimately requisitioned by allied forces. Those that remained in Danish waters were primarily used to carry German coal and coke to Denmark. A total of 25 Maersk ships were wrecked during the war, and 150 seafarers lost their lives. Thanks to fast rebuilding and the acquisition of larger vessels, Maersk was able to restore its operations and expand its business adding new routes.

In the 1950s, Maersk expanded its operations to include tanker shipping, which involved transporting oil and gas around the world. In 1956, the company launched its first container ship, the "Emma Maersk", which was one of the largest container ships in the world at the time. This move revolutionized the shipping industry and helped to reduce the cost and time required for transporting goods.

In the 1990s, Maersk expanded into other industries, such as the oil and gas industry, where it focused on exploration and production. The company also entered the offshore drilling industry, which involved drilling for oil and gas in deep waters. In addition,

Maersk expanded into the logistics industry, providing freight forwarding, supply chain management, and other services to customers around the world.

Following a strategic review in 2016, it was announced that A.P. Moller - Maersk would reorganise into two separate divisions: Transport & Logistics and Energy, with the purpose of becoming a focused integrated transport & logistics company.

By 2017, Maersk became a global leader in the shipping and logistics industry. It played a major role in 343 ports around the world managing about 18% of the world's container shipping, meaning that *"every 15 minutes on average a container ship will come to a port somewhere with between 10 to 20 thousand containers". "For each container shipped, there may be up to 30 different parties involved, communicating up to 200 times"* (Maersk Annual Reports; World Economic Forum, 2018).

At the time, the company's core business was ocean shipping, which involved transporting goods and cargo by sea for customers around the world. Maersk operated a large fleet of container ships, tanker ships, and other vessels, with a total capacity of around 4 million TEUs (twenty-foot equivalent units).

Despite its success, Maersk had to face a number of challenges over the years. On 27 June 2017, the company was hit by the NotPetya cyberattack [See Insight Box 2], which caused widespread disruption to its operations and resulted in losses of over $300 million. The attack forced the company to shut down its IT systems and disrupted business operations at many of its ports around the world (World Economic Forum, 2018).

While the origins of the attack are still not entirely clear, it is widely believed that it was launched from Russia and that it was intended as an act of sabotage against Ukraine. The attack occurred in the context of the ongoing conflict between Ukraine and Russia, which began in 2014 when Russia annexed Crimea and that featured a strong fighting between Ukrainian forces and Russian-backed separatists in eastern Ukraine [See Insight Box 1]. The conflict was marked by accusations of cyber attacks and disinformation campaigns by both sides. In this context, the Maersk attack can be seen as a side effect of the wider conflict, and as an example of the way in which cyber attacks can have unintended spill over effects to companies and individuals who are not directly involved in the conflict.

Maersk's response to NotPetya was widely regarded as effective and efficient given the scale

and severity of the incident which forced the company to rebuild its entire IT infrastructure from scratch. It took approximately ten days to restore its essential business systems, and several weeks to fully recover all its operations.

During the initial response, the company's priority was to restore its IT systems and minimize the impact on its customers. The company also brought in external IT experts and forensic teams to assist with the recovery effort, and it communicated transparently and frequently with its customers, employees, and stakeholders throughout the recovery process, updating them on the status of its operations and systems. In the days and weeks following the attack, Maersk conducted a thorough review of its cybersecurity measures and implemented a number of changes to strengthen its defenses. The company also shared its learnings from the attack with the wider industry and called for greater collaboration on cybersecurity issues (Greenberg, 2018).

Overall Maersk's response to the NotPetya attack has been widely praised as a model for other companies facing similar cyber attacks. The company's swift and decisive action, together with an unprecedented human resilience, helped to minimize the impact of the attack and restore operations as quickly as possible (Greenberg, 2018; Swinhoe and Editor, CSO, 2019; Wesley et al., 2019). The incident was an expensive and significant wake-up call. It stressed the need for education and diligence in promoting and practicing cyber hygiene and instituting robust cyber defenses (Capano, 2021).

Since then, Maersk has been working not only to improve its cybersecurity but also to make it a competitive advantage, together with the adoption and implementation of a strong digital transformation and innovation strategy. The company has launched a number of initiatives to improve its digital capabilities, such as creating a digital marketplace for shipping services and using blockchain technology to improve supply chain efficiency.

Today, Maersk is a global company with operations in over 130 countries and a workforce of around 80,000 employees. The company continues to evolve and adapt to changing market conditions and technological advancements, with a focus on sustainability, security and responsible business practices (Maersk Company Website).

INSIGHT BOX 1: Ukraine and the Cyberwar

Throughout its history, (der Loo, 2016; Lowe, 2013; Magocsi, 2012; Roessler, 2017; Welfens and Gavrilenkov, 2000) Ukraine has often been a battleground between eastern and western powers. In the 20th century, the country was occupied by both Poland and Germany to the west, as well as Russia to the east, with Ukrainians aligning themselves with various occupying forces during these conflicts. After the defeat of Germany by the Red Army at the end of the Second World War, Ukraine remained entirely under Soviet control for the next four decades. Despite this, the country experienced significant economic growth, leading the Soviet Union in output for key commodities and hosting technology centres for aerospace, energy, and weapons.

After the fall of the Iron Curtain, Ukraine gained independence in 1991, but struggled economically compared to other former Soviet republics due to hyperinflation and recession. State failures led to rise of the black market, and Ukraine remained heavily reliant on Russia, which accounted for almost 40% of its trade. Tensions between Ukraine and Russia over economic and political affairs reached a boiling point in 2013 when anti-government forces rose against pro-Russian president Victor Yanukovych. Yanukovych sought to strengthen Ukraine's ties with Russia, while many Ukrainians wanted closer ties with the West and potential European Union membership.

In 2014, Russia annexed Crimea following an uprising by pro-Russian militias, while other parts of eastern Ukraine attempted to secede, with pro-Russian separatists receiving support from Moscow. Despite these challenges, Ukraine continued to integrate with the West, signing free-trade and visa-free travel agreements with the European Union in 2016 and 2017, respectively, as steps towards potential membership.

The period following the annexation of Crimea by Russia in 2014 was characterised by sustained and disruptive cyber-attacks against key Ukrainian infrastructure by Russian-sponsored groups. In November 2015, the Ukrainian power grid was hacked by groups allegedly linked to Russia, causing a widespread power blackout (OBR Office for Budget Responsibility, 2022). The successful attack in 2015 was followed up by the NotPetya ransomware attack of 2017 where the total cost of the attack was estimated at nearly $10 billion globally. The White House dubbed the attacks as the *"most destructive and costly cyber-attack in history"* (The White House, 2018).

INSIGHT BOX 2: NotPetya Ransomware Attack

NotPetya ransomware, recognised in 2018 as the second global information security issue in the world, is a modified version of Petya that is referred to as NotPetya to distinguish this attack from the old version of Petya attacks (Fayi, 2018). The NotPetya ransomware was characterised by some distinctive features that, as stated by Craig Williams, director of the Cisco division that reversed engineer and analysed the ransomware, made it *"simply the fastest-propagating piece of malware we've ever seen. By the second you saw it, your data center was already gone"* (Fayi, 2018; Greenberg, 2018; Menshawy, 2019; Newman, 2018; Sood and Hurley, 2017; Wesley et al., 2019).
Said features are:

- **Infection vectors**: NotPetya was primarily spread using a malicious update of the Ukrainian tax preparation software called M.E.Doc. The malware was also able to spread through other channels, including email attachments and network shares.
- **Propagation**: NotPetya was able to propagate itself laterally across networks, infecting other computers and systems connected to infected machines. The malware was able to exploit various

vulnerabilities in the Windows operating systems, including EternalBlue, PsExec, Windows Management Instrumentation (WMI), and EternalRomance to propagate quickly through the infected network.

- **Encryption**: Unlike typical ransomware, NotPetya did not actually encrypt the files on victims' computers. Instead, it used a technique called "disk-level encryption," which encrypted the master boot record (MBR) and the file system tables on infected systems, effectively rendering them unusable. Additionally, although it still purports to be ransomware, the encryption routine was modified so that the malware could not technically revert its changes. Despite offering to restore infected computers after having paid a ransom of 300$, there was no mean to pay it or receive decryption keys.
- **Persistence**: NotPetya was designed to persist on infected systems, even after a reboot. The malware used a number of techniques to ensure that it would remain active, including the use of scheduled tasks and the creation of a new user account with administrative privileges.
- **Impact**: While the initial infection vector for NotPetya was traced back to Ukraine, the malware was not specifically targeted at Ukrainian companies or organizations, and it did have significant consequences for businesses in many other countries including Russia, the United States, European countries and India. More than 300 Ukrainian companies were compromised, accounting for roughly 10% of the countries' computers. Additionally, all the multinational corporations maintaining business relationships with the region and using the M.E.Doc tax system were infected, allowing NotPetya to rapidly spread throughout their global networks.
- **Attribution**: The attack was initially believed to be a form of financial cybercrime, as the ransomware demanded payment in exchange for access to encrypted files. However, later analysis indicated that the attack may have had political motivations, as the malware was designed to destroy data rather than simply encrypting it. Some experts have suggested that the attack may have been carried out by a state-sponsored actor, possibly with links to the Russian government. The NotPetya attack was indeed the first time Western officials publicly attributed a cyber attack to groups linked to the Russian government, with the National Cyber Security Centre NCSC in the UK releasing a statement to this effect in 2018 (NCSC National Cyber Security Center, 2017).

Overall, NotPetya was a highly sophisticated and destructive piece of malware, designed to cause widespread disruption to targeted systems and networks. Its use of disk-level encryption and lateral propagation techniques made it particularly effective at infecting and disabling large numbers of systems. Its impacts were devastating.

The NotPetya cyberattack was not directly related to the ongoing conflict in Ukraine, but it did have significant consequences for businesses and organizations in Ukraine and other countries as well. Maersk was one of the most high-profile victims of the attack, with the company reporting losses of up to $300 million. The attack caused significant disruption to Maersk's global operations, with many of the company's systems and communications channels being taken offline or compromised.

NotPetya highlighted the vulnerabilities of critical infrastructures and supply chains to cyber threats. The attack served as a wakeup call for businesses and governments around the world, leading to increased investments in cybersecurity and greater awareness of the risks posed by cyber threats.

3.4 Data Collection

To build the narrative and proceed with the analysis of the Maersk case study, multiple sources of data were used, including interviews, podcasts, documents and papers. It is important to emphasise that the narrative was not based on direct interviews, due to the impossibility of interviewing the company's personnel involved in the case. However, as with the reference paper, this did not pose a limitation to the conduct of the analysis.

In fact, as explained in section 3.2, the chosen case presents a large amount of public information and testimonies released by the top managers directly involved in all the activities conducted during the cyber attack. Many of them participated into panel discussions, interviews and podcasts in which they had the possibility to describe the attack from their own perspective and share their personal opinion on what happened. These testimonies represented very valuable data which were used as the primary source to reconstruct the narrative. In addition, also some secondary data were selected in order to give a more detailed overview of the attack which was essential to conduct a thorough analysis.

All the sources used for the narrative are listed in Figure 3.2 and are divided into primary and secondary, depending on whether they contain or not passages reported directly by one of the Maersk's managers or employees. In particular, the primary data include all the references in which a relevant employee of Maersk playing an active role during the NotPetya attack, had the possibility to share his own perspective of what happened. Said employees are:

- Jim Hagemann Snabe, Maersk Chairman who referenced to the NotPetya attack in a panel discussion on securing the future of cyber space at the World Economic Forum, 2018;
- Soren Skou, Maersk CEO who was interviewed by the Financial Times in 2017 on the cyberattack;
- Gavin Ashton, Maersk Identity & Access Management (IAM) service owner who wrote a post on his personal blog in which he described in details what happened during the attack. Moreover, together with Bharat Halai, Maersk head of Identity & Access Management, he was the protagonist of the fourth episode of the Bank

Infosecurity podcast series "The Ransomware Files" focused on describing how Maersk faced the attack;

- Adam Banks, Maersk CTO & CIO who gave a key note speech during InfoSecurity Europe 2019 focused on the NotPetya attack;
- Andy Powell, Maersk CISO who was the protagonist of the Episode 438 of SE-RADIO podcast in which he described the lesson learned from the attack.

Using the same approach of the reference paper, these testimonies are quoted during the analysis using the initials of each representative's name as indicated in the third column of Figure 3.2.

DATA COLLECTION			
Source	**Type of Data**	**Person involved**	**Referred to as**
Primary	Panel discussion on Securing the future of cyberspace at the World Economic Forum during WEF. January 24, 2018	Jim Hagemann Snabe, Maersk Chairman	{JHS}
	Financial Times interview "Maersk CEO Soren Skou on surviving a cyber attack". August 13, 2017	Soren Skou, Maersk CEO	{SS}
	Post "Maersk, me & NotPetya" on the personal blog page of Gavin Ashton	Gavin Ashton, Maersk Identity & Access Management (IAM) service owner	{GA}
	Keynote speech, InfoSecurity Europe 2019	Adam Banks, Maersk CTO & CIO	{AB}
	Episode 4 of Bank InfoSecurity series "The Ransomware Files" - "Maersk and NotPetya, Malware Disguised as Ransomware Nearly Sank Logistics Giant Maersk". January 25, 2022	Gavin Ashton, Maersk Identity & Access Management (IAM) service owner Bharat Halai, Maersk head of Identity & Access Management	{GA}/{BH}
	Episode 438 of SE-RADIO "Andy Powell on Lessons Learned from a Major Cyber Attack". December 12, 2020	Andy Powell, Maersk CISO	{AP}
	Keynote speech at Black Hat Europe December 2-5, 2019, on "Implementing the Lessons Learned From a Major Cyber Attack"	Andy Powell, Maersk CISO	{AP}
Secondary	Episode 54 of Darknetdiaries "NotPetya"	NA	NA
	Article by Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History". Wired August 24, 2018	NA	NA
	Case Study: "Cyberattack: The Maersk Global Supply-Chain Meltdown". Ivey Publishing. September 4, 2019	NA	NA
	Company website, Company official twitter account, and Company annual reports from 2016 to 2021	NA	NA

FIGURE 3.2: *Sources used for reconstructing the narrative of Maersk case*

It is worth to emphasise that the references chosen involve people holding different positions

in the company entailing different responsibilities and routines, both in the case of normal activities and during a crisis. Moreover they all played a key role in the response to the attack during which they were involved on different fronts and in which they were called upon to complete different tasks. Thus, their testimonies provide a 360-degree perspective of what happened, guaranteeing the validity and completeness of the narrative constructed.

To complete the narrative, and in order to provide more details on the development of the events, several valuable secondary sources were also used, including official web pages, case studies and articles. Finally, Maersk's annual reports from 2016 to 2021, and Maersk's official Twitter account were also analysed as they were useful to understand any changes in the company's strategic, organisational, and financial plan in response to the attack.

3.5 Data Analysis

The construction of meaning from collected data was the result of a progressive data analysis procedure that, through the adoption of several inductive steps, allowed to go from data to theory development.

According to the literature, the process of qualitative data analysis involves immersing oneself in the data collected and consolidating it by focusing on segments that could potentially provide insights into the research questions. The researcher then must compare these segments to identify patterns and themes, interpreting what was said and making meaning from them. These interpretations become the findings of the study. Essentially, qualitative data analysis is the process of making sense of the data (Williams and Moser, 2019).

While there is no standardized procedure for conducting qualitative data analysis, various narrative researchers have published guidelines and processes for analyzing narratives. Among them, the procedure chosen and used in this thesis is the same adopted by the authors of the reference paper, namely the *narrative thematic analysis*. In this approach, content within text is considered as the primary focus to investigate the collected data (Butina, 2015).

The narrative thematic analysis consists of five stages:

1. Organizing and preparing the data collected
2. Obtaining a general sense of the information
3. Performing the coding process
4. Categorising into themes
5. Interpreting the data

The remaining subsections of this chapter will be entirely devoted to describing how the first four steps of the analysis were performed. The next chapter will be focues on providing a thorough explanation and interpretation of the themes and the categories found.

3.5.1 Organizing and preparing the data, and Obtaining a general sense of the information

The initial stage of the analysis was *organizing and preparing the data* and it first involved transcribing audio recordings of the podcasts, key note speeches and panel discussions. In this phase any non-narrative lines, like casual conversation, and any contribution by other guests or speakers were excluded. During the transcription process, basic patterns or themes were identified and noted in the margins of the transcript. The transcripts were then stored into a unique repository which was finally completed with additional quotes and sections taken from the selected secondary sources of data previously described.

The second step of the investigation was *obtaining a general sense of the information.* For completing it, it was essential to read and re-read the collected and prepared data to gain familiarity with the content. Passages and citations where organised and grouped according to the phase of the crisis to which they referred (before, during or after). This was particularly helpful to understand the key features for each of the three different stages in terms of crisis management, response activities and leadership competencies.

This step also involved taking notes and making observations about the data, identifying recurring themes and patterns, and developing an initial coding scheme. Relevant passages and sentences were highlighted, underlined and commented. Multiple recursive themes and concepts emerged, and they were noted down. This allowed to familiarize with the data and to start having a good feeling and understanding of the main distinctive aspects that characterised Maersk response to the NotPetya cyber-attack.

3.5.2 Performing the coding process, and Categorising into themes

The subsequent stages after organizing, preparing and getting a general sense of the data were the *manual coding process* and the *categorization into themes*. While automatic qualitative analysis software programs are available to perform these activities, for this thesis the analysis was done manually in order to keep full awareness and control of all the steps. This was essential to derive relevant findings and respond to the research question.

Coding was defined by Glesne as a *"progressive process of sorting and defining and defining and sorting those scraps of collected data...that are applicable to your research purpose"* (Glesne, 2006).

According to the literature, the coding process is an essential part of qualitative data analysis, which involves the recursive identification of themes and patterns within the data. It is characterised by three subsequent steps:

1. **Open coding**: Open coding is the initial level of coding where the researcher identifies and categorizes distinct concepts and themes. This process involves reading through the data and identifying concepts, themes, and patterns that are present. The data is organized by creating initial broad thematic domains for data assembly, known as *First Order Concepts - FOCs*.
2. **Axial coding**: Axial coding, as the second level of coding, involves further refining and categorizing the emergent FOCs from the first level of coding. Unlike open coding, axial coding aims to identify relationships between the open codes and develop core codes that represent the most closely interrelated themes, the so called *Second Order Themes - SOTs*. The goal of axial coding is to create distinct thematic categories that will guide the selective coding process. *"Axial coding identifies relationships between open codes, for the purpose of developing core codes. Major/core codes emerge as aggregates of the most closely interrelated or overlapping open codes for which supporting evidence is strong"* (Strauss, 1987).
3. **Selective coding**: Selective coding is the third stage of coding in qualitative research. Its purpose is to synthesize and integrate categories from axial coding into meaningful expressions. Selective coding takes the process of axial coding a

step further by identifying the core themes that connect the categories, the so called *Third Order Themes - TOTs*.

Following these three steps, the coding process for the analysis of the Maersk Case involved re-reading the transcripts to identify recurring words, ideas, or patterns from the data. Prominent ideas and recurring words/messages were highlighted within each narrative and corresponding FOCs where developed. Those concepts were placed in the margin and then transcribed into an excel file where they were grouped according to the stage of the attack they were referred to. In total 67 FOCs were denoted. The axial coding step was then applied and 22 SOTs where identified. These themes were then grouped into 9 logical categories, the TOTs, that reflected the major findings of the study (see Figure 3.3). Figure 3.4, Figure 3.5 and Figure 3.6 show the entire coding procedure organised according to the three different stages of the crisis management: pre-crisis, during-crisis and after-crisis.

AXIAL CODING - *Second Order Themes*	SELECTIVE CODING - *Third Order Themes*
Lack of information sharing among company levels	collaboration deficit
lack of training and awareness	organizational ignorance
lack of guidelines, measures, procedures	technical ignorance
lack of visibility	effective decision making under risk and preassure
top management ignorance	network leverage
inadeguate technical tools	open and ethical communication
effective decision making	organizational agility and creativity
prioritization of activities	organizational learning
risk taking	organizational implementation
work under pressure	
cooperation and involvement of external stakeholders	
ethical behaviour	
open and transparent communication	
empowerment of people	
human resilience, hard work and commitment	
creativity	
need of cultural change	
need of skills, tools and capabilities	
definition of cybersecurity strategy	
reorganization of processes	
skills & capabilities developement	
talent acquisition	

FIGURE 3.3: *Second Order Themes and Third Order Themes resulting from the coding process applied to the Maersk case*

STAGE OF CRISIS	OPEN CODING *First Order Concepts*	AXIAL CODING *Second Order Themes*	SELECTIVE CODING *Thrid Order Themes*
PRE - CRISIS	Lack of dialogue between top management and operative levels	lack of information sharing among company levels	collaboration deficit
	Difficulty for IT staff to communicate the relevance of vulnerabilities in the system to decision makers		
	Security best practices were not followed by employees at all company levels	lack of training and awareness	organizational ignorance
	Company-wide lack of awarness in cybersecurity		
	Lack of company-wide education and training in cybersecurity		
	Lack of company guidelines or procedures to follow in case of IT anomalies / cyber-attack	lack of guidelines, measures, procedures	
	Insufficient cybersecurity measures in place to protect the infrastructure		
	Lack of cyber crisis management plan		
	Lack of company-wide consistent security baselines and policies to be followed in daily activities to ensure cyber-physical security		
	Lack of business continuity plan before the crisis		
	Lack of understanding of the threat landscape - (geopolitical scenario and vulnerabilities due to complex supply chains were not considered)	lack of visibility	
	Lack of visibility of the entire infrastructure and of its critical applications/processes		
	Security was not a relevant KPI to achieve bonuses	top management ignorance	
	Strong digital trasformation strategy in place without adeguate attention to cybersecurity implications		
	Lack of dedicated team to cybersecurity - lack of CISO		
	Security did not receive enough attention by leadership team		
	IT considered by top management as a cost to be minimised, not as an enabler. Not considered as critical component of the company		
	Lack of tools technologies supporting cybersecurity operations	inadeguate technical tools	technical ignorance
	Insufficient technical tools to support digitalization strategy		
	Sub-optimal backup strategy for relevant data, not considering all possible scenarios (lack of creativity)		

Figure 3.4: *Results of the coding process applied to the Pre-Crisis phase of Maersk case*

STAGE OF CRISIS	OPEN CODING *First Order Concepts*	AXIAL CODING *Second Order Themes*	SELECTIVE CODING *Thrid Order Themes*
DURING - CRISIS	Initial general confusion due to complete unpreparedness about the situation	lack of training and awareness	organizational ignorance
	Lack of understanding of the source of the attack when the crisis started	lack of visibility	
	Initial lack of understanding of the impacts and victims of the attack		
	Initially no information/guidelines to follow shared by HQ with the company's terminals and ports	lack of information sharing among company levels	collaboration deficit
	Effective and quick decision making particularly by top management	effective decision making	effective decision making under risk and preassure
	Prioritization of activites to be completed to restore operations and achieve quick wins - priority given to business critical processes	prioritization of activities	
	First objctive pursued: understand the cause of the attack and attribution		
	Decision making under uncertainty without waiting everything is perfect	risk taking	
	Ability to work under pressure	work under pressure	
	Consistent and disciplined approach and calmness demostrated by top management		
	Direct involvement and cooperation with consultancy Deloitte and with smaller IT firms with no budget limits providing required competences	cooperation and involvement of external stakeholders	network leverage
	Direct involvement, cooperation and support from partners, suppliers and customers		
	Open and trasparent customer relationship management to safeguard their loyalty	ethical behaviour	open and ethical communication
	Extraordinary effort by top management to protect employees and safeguard them during the crisis		
	Strong company culture and values		
	Consistent, transparent and open external communication with customers, partners and contractors	open and transparent communication	
	Regular release of public updates to inform customers and external stakeholders about the ongoing situation		
	Open, frank and honest communcation with internal employees		
	Delegation of responsability and decision making power of people on the front line	empowerment of people	organizational agility and creativity
	Heroic effort of employees working 24/7, human resilience, hard work and commitment	human resilience, hard work and commitment	
	Real team effort and commitment to continue operations		
	Use of creative and out-of-the-box tools and solutions to solve challenges (whats-app, pen and paper, manual workaraounds, ...)	creativity	

FIGURE 3.5: *Results of the coding process applied to the During-Crisis phase of Maersk case*

STAGE OF CRISIS	OPEN CODING *First Order Concepts*	AXIAL CODING Second Order Themes	SELECTIVE CODING *Third Order Themes*
AFTER - CRISIS	Recognition of the fact that a cyber attack cannot be fully avoided, thus resilience and business continuity have to be developed	need of cultural change	organizational learning
	Protection is not enough. A balance of reactive and proactive approach is essential to effectively face a cyber attack		
	Cybersecurity has to become a competitive advantage		
	IT unit is not a cost but a business anabler		
	Stronger engagement, collaboration and trust is needed between top managers and company employees		
	Empowerment and agility were fundamental to allow recovery		
	Basic procedures and guidlines in cybersecurity have to be introduced and followed		
	The threat landscape has changed: new state sponsored cyber attacks and increased vulnerability surface		
	Training and learning activity are needed to be ready to face a cyber-attack	need of skills, tools and capabilities	
	Acquiring visibility of the external context and of the internal critical processes is essential to be able to counter cyber threats		
	Soft skill and lateral thinking are essential to face cyberattacks		
	Investments in offline backups of critical processes are required		
	Strong investment on cybersecurity to improve cybersecurity posture	definition of cybersecurity strategy	organizational implementation
	Definition of cybersecurity strategy, policies and guidelines		
	Holistic approach to cybersecurity strategy and balance of investments in containment, application vulnerability fix, and recovery measures to be implemented		
	Prioritization of investments in cybersecurity using a risk-based approach		
	Developement of forensics capabilities and tools to learn and share the insights with the ecosystem	skills & capabilities developement	
	Deployment of tools and technologies to ensure security of Mearsk infrastructure		
	Continuous exercise and training for the entire company population		
	Redesign of company processes according to groups that worked best during the crisis	reorganization of processes	
	Adoption of secure-by-design and resilience approach		
	Creation of security team lead by an expert CISO to design cybersecurity startegy aligned with the company digitalization strategy	talent acquisition	
	Adoption of read team made of young people to constantly test the organization and find new vulnerabilityes		
	New young talent acquisition and diverse experts with original ideas and lateral thinking and creativity to test the company and find new vulnerabilities		
	After full recovery, constant information sharing on cybersecurity and lesson learned with all stakeholders	cooperation and involvement of external stakeholders	network leverage

Figure 3.6: *Results of the coding process applied to the After-Crisis phase of Maersk case*

4 Analysis

This chapter is entirely devoted to present the *data interpretation*, which is the last step of the narrative thematic analysis started in Chapter 3. In this last phase, the third order themes that were identified after performing the coding process (see subsection 3.5.2) were used as the starting point to analyse and interpret the Maersk case. Given the research objective, during the investigation a particular focus was given to understand how the crisis was handled by Maersk's top managers and its key employees, and on the leadership competencies that were used or that were missing.

As for the structure of the chapter, the first section will be used to give a general overview of the attack with a focus on its technical aspects so to provide a comprehensive framework which is useful to better understand the analysis. This will also allow to better contextualise human behaviours and reactions. Then, the remaining sections will be dedicated to present the analysis performed for each of three crisis management phases (before, during and after the attack).

4.1 Overview of the attack

Maersk was hit by the NotPetya ransomware on June 27, 2017. One single infection was responsible for the Maersk compromise - the MeDoc software that had been installed on a company computer in Odessa, a Ukrainian port city on the Black Sea; it was all the malware needed to infect the entire system. As a result, Maersk's entire booking system went down, and its complex loading infrastructure used to systematically load container ships to avoid capsizing them were also affected.

"It was the end of June, a nice, summer day. The morning started out like any other. The planned meeting began and discussions about the new Managed Service operations had just commenced, when a large commotion spread across the office. Suddenly, the monitoring screens started to show all systems turning to red, and not long after all laptops started to reboot" (Predica, 2018).

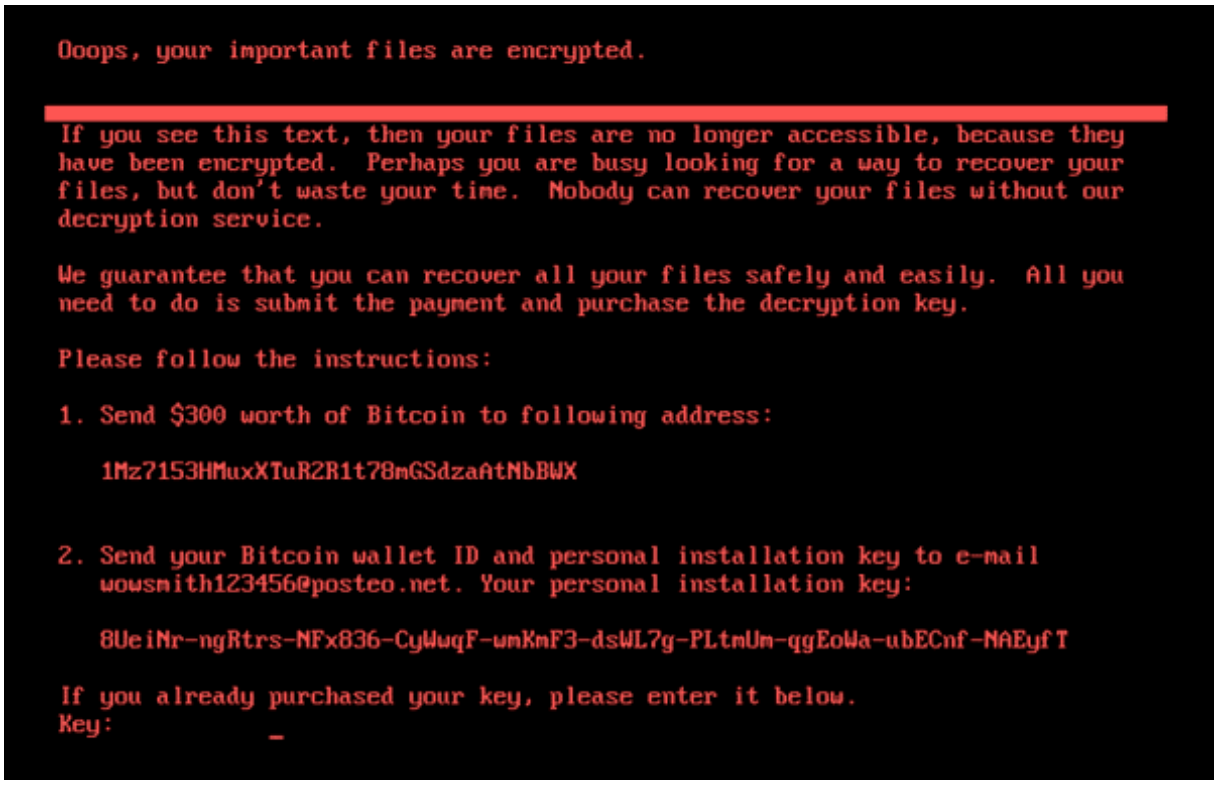


Figure 4.1: *A message demanding money on a computer hacked by NotPetya in June 2017. (Source: G. Ashton. "Maersk, me & notpetya" personal blog)*

Maersk's incident response team immediately assembled an emergency recovery center in

the London headquarters to mitigate and recover from the NotPetya attack, which required hundreds of staffers working 24/7 to rebuild the network. All computer equipment was confiscated, and new computers were obtained and then distributed to recovery personnel. Staff began rebuilding servers from the ground up. However, the effort came to a halt when it was discovered that there was no clean backup of the company's domain controllers.

A domain controller is a server that handles authentication and verification requests for user access to network resources. Maersk had around 150 domain controllers within its global system, which would have normally synced with each other to become a backup for a compromised or damaged server. This decentralized backup strategy would have allowed for fast recovery from a localized event. However, no one had envisioned a scenario where all domain controllers would be wiped out in a massive attack, rendering the network useless. Fortunately, Maersk's staff found a pristine backup in their Ghana office. A power blackout had disconnected the server from the network, saving it from the NotPetya attack. The backup contained a single clean copy of the company's domain controller data and was a relief for the recovery team.

Getting the data to the recovery center was challenging due to poor network infrastructure in Ghana, and the available bandwidth was low. The backup consisted of several hundred gigabytes of data, and it would take days to transmit it to the recovery center. Flying a staff member to London was not possible, so the backup was hand-delivered to a Maersk employee in Nigeria, who then flew back to Heathrow. Once in the headquarters, this unique backup became the first block of the new network that had to be created.

While the IT staff was working around the clock to rebuild the entire network, the company had to manage shipments manually. As a result, Maersk's shipping volume declined by 20%, and customers were forced to resort to pen and paper to track their packages. Fortunately, the company's ships were mostly disconnected from the network during the attack and were able to function independently. Once the network restoration began, online ordering and tracking was prioritized. The recovery team focused on bringing up Maersk's core services, especially port services. Reading a ship's inventory was indeed crucial in determining where the containers were and where they were headed. The booking system came back online later, and it took at least two weeks for port facilities to operate normally again.

Maersk estimated that NotPetya cost the company between $250 million and $300 million

in expenses and lost earnings. In addition, any locally stored information on infected PCs that had not been backed up prior to the attack was forever lost, including contacts, orders, and personal files.

4.2 Before the crisis

The before-crisis period covers all Maersk's activities starting from 2015 until the cyber attack took place on June 27, 2017. Three Third Order Themes have been identified for this stage of the crisis, namely:

1. Collaboration deficit
2. Organizational ignorance
3. Technical ignorance

All of them highlight that the company, prior to the crisis, was experiencing a general unpreparedness both from the organizational perspective and from the technical one.

In the years preceding the cyber crisis, Maersk had started a strong digital transformation to redesign its processes and increase its competitiveness. As {GA} stated, at the time *"... The energy businesses were sold off to consolidate core functions – shipping and logistics, IT was centralised, a digital and cloud-first strategy was established at the very highest level of the organization"*.

However, this strong digital strategy was missing some major aspects, primarily from the organizational perspective where managers were not fully aware of the risks and consequences associated to it. Challenging strategic objectives where set to unlock the opportunities of the digital world, but no proper investments were made to guarantee the adoption of the adequate tools and technologies needed to support the transformation, and no procedures, policies or processes necessary to guide it were defined or developed.

As a result, **technical ignorance** was a very critical issue at the time. {GA} declared that *"we had limited systems to work with. I'd regularly be up until 4am running tests of various kinds with systems hopelessly underspecified for the job"*. This lack of proper technical tools to support the digital transformation strategy of the company sensibly contributed to increase its vulnerability surface. In addition, no tools and technologies

were in place to secure the new cyber-physical infrastructure of the company. Moreover, suboptimal backup strategies were in place, as they did not take into account all the possible scenarios that could have occurred in case of a physical or cyber attack.

Furthermore, the technical ignorance was further amplified by the **ignorance at the organizational level**. At the top management, there was a general lack of awareness about the importance of defining a solid cybersecurity strategy that had to be embedded into the digital one. Only this approach would have enabled Mearsk managers to properly assess the risks related to the adoption of the new technologies.

This was evident from the words of {GA}, who wrote *"my next target was privileged access. Securing the keys to the kingdom. During the previous project I had noticed all kinds of gaps. Essentially, the principle of least privilege was not generally followed. Shipping is a huge business but operates on relatively thin margins. IT had up until that point had been managed as a cost centre to be minimised, rather than as a business enabler. In the race to the bottom, security controls had ultimately suffered and become a secondary concern to delivery. With the historical organisational structures within IT, we had multiple security functions with no clear lead, and limited funding"*. Moreover, he stated *"They had differing levels of maturity when you looked at different layers of the IT stack. In the days gone by, you operated in a four-walls environment, you had your data center, your office block, and you'd focus on your network layer, on your firewalls and you keep yourself in your little box - that doesn't really work anymore, which was one of the things that NotPetya really highlighted"*.

This makes it clear that the top management considered security and IT as a cost to be minimised rather than a business enabler. In fact, security was not a relevant KPI to achieve bonuses causing all the activities related to securing Maersk's network to be widely disregarded. There was no clear strategy to define the cybersecurity activities to be put in place to protect the company, eventually leading to strategic choices that used to limit as much as possible investments in cybersecurity and IT, in order to increase spendings on other activities that at the time were considered as core for Maersk competitive advantage.

This very same concept was highlighted also by {AP} who stated *"two and a half years ago [Maersk] was like the rest of the shipping companies in the logistics and supply industry in terms of its maturity, it sat pretty low on the sector maturity scale. At the top, the banks*

and the governments who've spent a lot of time and money on protecting what they've got. In the middle we had primarily the sort of the retail business, and closer to the bottom we had the manufacturing and we had the logistics supply type capability. So we were very similar to most of our competitors and most of the industry at the time, in that the IT network was not at the time considered a critical part of the company. It supported company operations in the mindset of most of what they did. But really it was an asset-focused company like most. It was about ships, it was about ports, it was about containers".

This ignorance at the managerial level had a domino effect on the entire company, generating diffused lack of cyber awareness at all the different hierarchical levels. There were no pre-defined company-wide guidelines, policies or procedure to be followed both in ordinary times and during organizational crisis. {GA} stated *"At Maersk, there had been no consistent security baselines. Some vague written policies existed but were frankly, largely ignored [...]. The lack of standardised and consistently applied privileged access controls, made it trivial for notPetya to wipe Maersk out."*

Furthermore, no cyber crisis or business continuity plans were present, and no specific training and educational activities were carried out to ensure preparedness of the company population in case of out-of-the-ordinary events.

The fact that Maersk's top management neglected cybersecurity and its potential impact on the company, also affected its ability to take into account all the possible factors threatening the company people, processes and technologies. There was indeed a severe lack of visibility on how the different components of the infrastructure were interrelated. There was no clear awareness on which were the core functions and assets that had to be prioritised, and there was a very limited understanding of the geopolitical context surrounding the company, that could have undoubtedly helped Maersk to prevent or mitigate the effects of NotPetya attack.

Finally, during the analysis of the before-crisis stage the theme of **collaboration deficit** among different stakeholders in the organization also emerged. A diffused lack of dialogue and information sharing between top management and operative levels, was indeed experienced in all the business units of Maersk. This resulted into the IT staff experiencing strong difficulties in communicating to decision makers the relevance of vulnerabilities in the system. Quoting {GA}: *"Cue two years of fruitlessly pushing for privileged access*

controls. In that time, we could and should have been in the process of applying consistent security policies to control accounts and access. [...] In the back of my mind, something a little more industry-grade was necessary, but with the focus on cost reduction being hammered home, this was simply wishful thinking. I didn't have millions in my back pocket!", and he continued *"The controls I'd been evangelising, could have saved Maersk from the impact. But I'll bet I wasn't the only one feeling responsible for this. And I absolutely didn't get the impression that any fingers were pointing in my direction, far from it. The following few months were going to see a flurry of activity, with the kinds of measures I had been looking to deploy since I joined the company all getting the green light. People were finally listening. It's amazing, the doors a good cyber-attack opens".*

From these words it is evident that the lack of collaboration and information sharing prior to the attack, caused managers to consider IT and cybersecurity spendings as not relevant for improving Maersk's organizational performance, and thus as not requiring time, attention and most importantly economic resources to be dedicated.

Overall, the technical and organizational ignorance, together with the lack of proper communication, caused Maersk to become a very vulnerable company with an immature cybersecurity posture, where the high degree of risk exposure was not properly mitigated by a well-structured cybersecurity strategy.

4.3 During the crisis

The proper crisis started on June 27, 2017, when the Company publicly declared on its official Twitter account that it was *"hit as part of a global cyber attack named Petya"* [see Figure 4.2]. {JHS} said *"I'll never forget, it was the 27 June when I was woken up at 4 o'clock in the morning. A call came from the office that we had suffered a cyberattack. The impact of that is that we basically found that we had to reinstall an entire infrastructure, we had to install 4.000 new servers, 45.000 new PCs, 2.500 applications".* The crisis lasted almost one month. Finally on July 25, 2017 Maersk published a global update on his website stating that the company was near to full recovery and that the majority of its global applications were back online and running [Exhibit 5 in (Wesley et al., 2019)].

Six Third Order Themes have been identified for this stage of the crisis, namely:

1. Organizational ignorance
2. Collaboration deficit
3. Effective decision making under risk and pressure
4. Network leverage
5. Open and ethical communication
6. Organizational agility and creativity

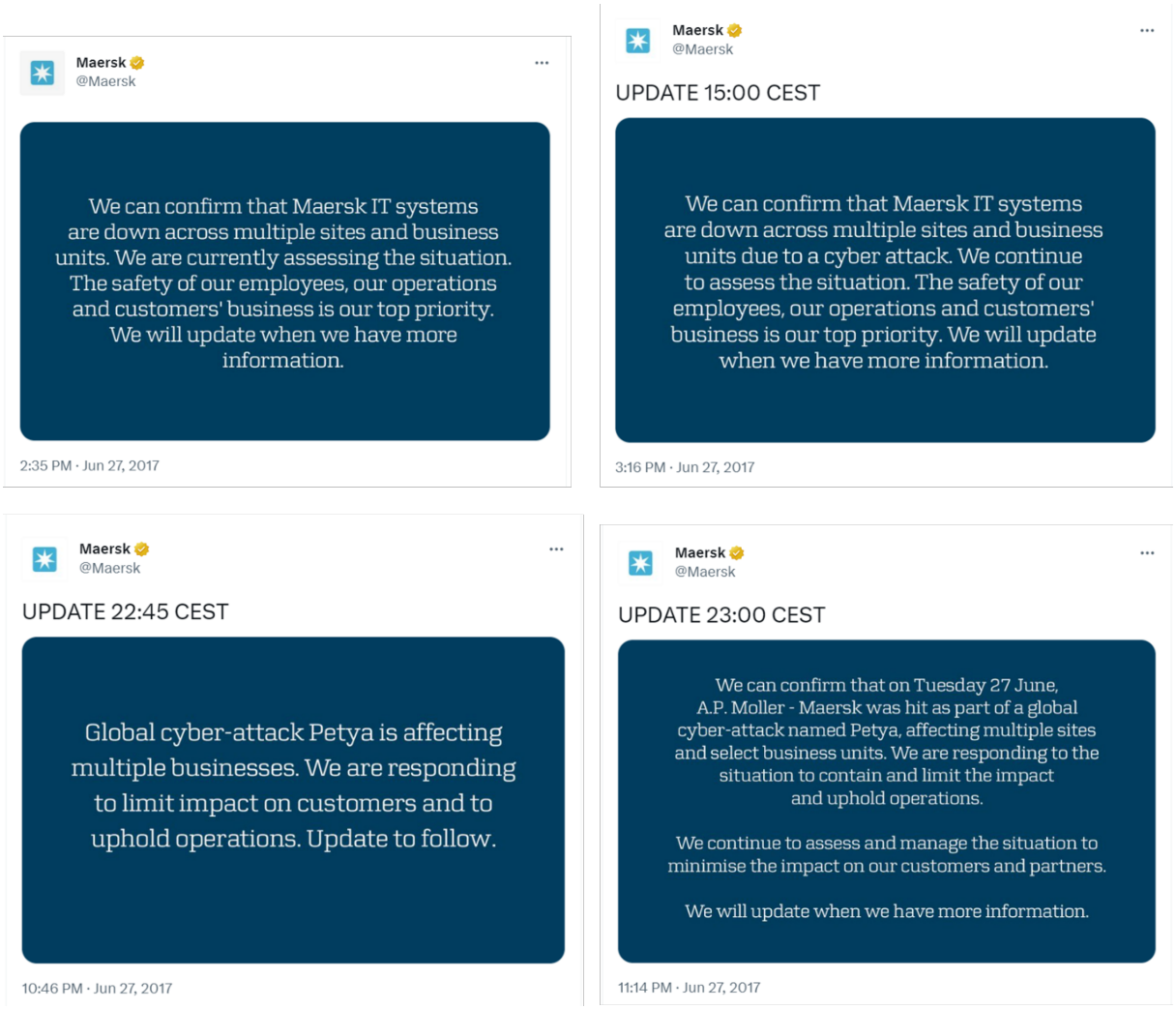


Figure 4.2: *Tweets posted by Maersk on June 27, 2017 (Source: Maersk official Twitter account)*

It is worth to notice that the first themes (i.e., organizational ignorance and collaboration deficit) are the very same theme found also in the analysis of the pre-crisis stage described

in the previous paragraph.

In fact, when NotPetya hit the company, Maersk was completely unprepared. The lack of established guidelines, training and awareness on how to face a cyber crisis resulted into an initial general confusion across all the business units around the world. The **organizational ignorance** of the top managers caused Maersk to be disoriented on what to do and on which activities to put in place to respond to the attack. As {SS} stated: *"Most business problems, you will have an intuitive idea on what to do. But with this and my skills, I had no intuitive idea on how to move forward"*.

It wasn't clear to them at first who was threatening the company or what, or why. There was so much chaos everywhere that it was impossible to get a realistic estimate of what was impacted and to which extent. This lack of awareness and visibility resulted into an **initial collaboration deficit** that was experienced among all the various stakeholders of the company. This lack of understanding experienced by the top management made it impossible to quickly provide guidelines to employees around the globe to explain what was happening and to instruct them on which actions to perform. This, together with the fact that the company also lacked any business continuity plan to put in place, caused employees to be left in the dark during the first days following the attack.

If at first the company was paralysed and shocked by the unprecedented cyber-attack, it was then immediately able to activate an optimal and efficient response thanks to a present and responsive leadership, ethical values and a resilient and committed workforce. In fact, when faced with this unprecedented crisis, even though at first they felt lost, Maersk's top managers rapidly took action to understand what was going on so to quickly react in order to minimize the impacts and restore the operations. *"To begin with, I was just trying to find out what was happening. It was important to be visible, and take some decisions"* stated {SS}.

One of the major themes that emerged in this phase of the crisis was indeed **effective decision making under risk and pressure**. Top managers got involved in every crisis call to keep informed and make critical decisions. The presence and visibility of leaders made a big difference in responding to the attack. Decisions were made in a very quick and efficient way with the primary objective being to achieve quick wins, even if that meant taking some risk without everything being perfect or complete understanding being

achieved.

Moreover, prioritization of activities was at the base of every decision to be made, so to prioritise business critical processes that were vital to guarantee the continuity of the main operations. {AP} declared *"the basic recovery period was in three phases. For the first three to four days was building, if you like, the central core again. We had to rebuild the central core of the network through the AD nodes. And then we had to, if you like, replicate that by buying all the laptops to restart the network. So, we bought most of the laptops in the UK, in India and elsewhere. And we then had to replicate what we had built also into the other various regions. That took us between nine days to two weeks. So that sort of length of time to get our core network and processes back up and running again".*

Throughout the analysis, it also appears that **open and ethical communication** and **network leverage**, were very critical and interrelated factors in navigating the crisis.

From the very beginning of the attack, Maersk adopted a very open and transparent approach toward its clients, partners and suppliers. Public daily updates were released, both on the website and using social networks, to inform the external stakeholders on the company situation and on what it was doing to respond to the attack. That allowed the company to maintain a single credible and consistent channel of communication avoiding the risk of diffusing contrasting and false information. *"In the case of the cyber-attack, Maersk was a model example in being open, frank and honest with the world about what was going"* {GA}. *"I think the most important thing was that Maersk was very transparent throughout the attack. We, unlike many companies who are hesitant time in those sense, we were very open both with our clients and customers, but also with our partners, you know, our technology partners in particular, we involved them"* {AP}.

Furthermore, being open and consistent in the external relations, allowed Maersk to receive help by its partners and customers, which were essential to create a synergic network of shared skills and competencies to respond to the attack. This is reflected in {AP} words: *"By telling our suppliers and our customers what was happening, straight away we got support. Really, really important. Microsoft were brilliant. They immediately leaned in to try and understand what was going on. But not surprisingly, they were a little bit shocked, as most of us, about what this was doing and how. okay, Microsoft were trying to help us develop patches as we went. But it was pretty clear that we were not going to be able to*

sort of counter what was going on. [...] the reality of life was the suppliers reached in to help us. Our main outsourced supplier is IBM. They were our main supporter running our data centres and a lot of our background capability. Microsoft, one of our key suppliers, all jumped, dropped everything and came to help us because we were open with them. Similarly, our clients started calling us. Clearly they were slightly worried about where their bananas were going to be. But the most important reason they started to call us, funnily enough, is we started telling them what was happening. Their first response was, how can we help?".

Also according to {AP} the strong relationship with their partners and customers was what really allowed Maersk to survive the attack: *"we wouldn't have been able to do that, to be honest, without the help of our partners. So we had IBM, as our main network partner who was superbly again, to help us. We had Microsoft. He did a great job helping us as well. So we wouldn't have been able to do it at that time at that scale, without the, of partners. Plus also the patients by customers".* The very same concept was highlighted by {AB}: *"During the attack, a number of the most significantly impacted businesses were in contact with each other at C-level to compare responses and to try to learn from each other. The media coverage helped this happen, as did a number of the large tech firms or consultancies. Due to the global scale of the attack, a number of key skills were in very short supply. Certain skills needed couldn't be sourced from tech firms or consultancies, so the media coverage allowed Maersk to reach out to partners, customers and suppliers who hadn't been impacted directly and borrow some of the key technical skills".*

Eventually, the strong relationship with external stakeholders allowed Maersk to minimise the impacts to its processes and operations, as highlighted by {JHS} *"We only had a 20% drop in volume, so we managed 80% of that volume manually. [...] Customers were great contributors to overcoming that".*

Continuing with the analysis, the next very important theme that emerged during this phase was **organizational agility and creativity**. The main factors that really allowed Maersk to face the crisis, despite being totally unprepared to it, were indeed human resilience, creativity and empowerment of people. These capabilities allowed employees to face the crisis bravely, with minimal impact on firm's activity.

In fact while the IT staff, together with external partners and suppliers, was working around the clock to rebuild the online network, Maersk's employees around the globe had

to go back to manual operations to keep the business running [see Figure 4.3]. Thanks to a brilliant set of soft skills, including lateral thinking and creativity, Maersk workers were able to resort to pen and paper to track containers, and personal Gmail accounts, WhatsApp and Excel spreadsheet were used to take orders and to communicate among each other and with customers.

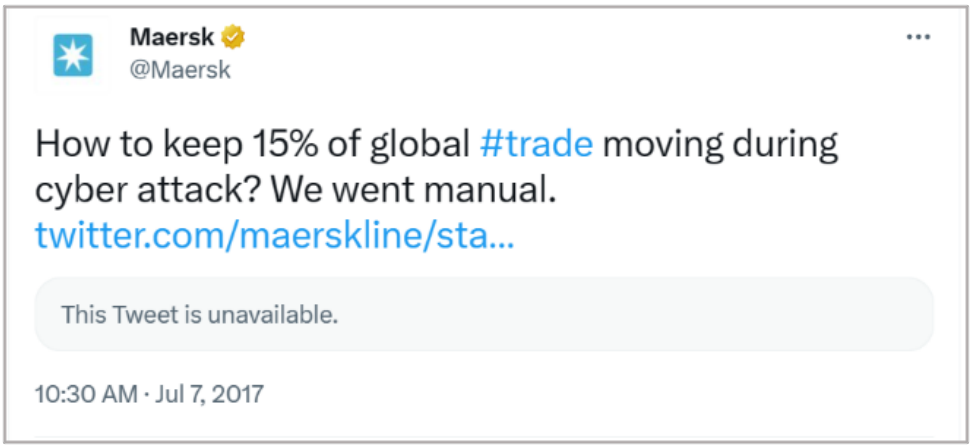


Figure 4.3: *Maersk Tweet on the effectiveness of manual operations during the crisis. (Source: Maersk official Twitter account)*

Furthermore, agility in responding to the attack was guaranteed also thanks to the delegation of responsibility and of decision making power to the front line employees. This allowed them to make quick and effective actions according to the present needs, without having to wait for the approval of the headquarters (HQ). *"Do what you think is right to serve the customer — don't wait for the HQ, we'll accept the cost"* {SS}. The same theme is expressed by {GA} statement *"The times immediately following The Event demonstrated the enormous value of getting the right people in a room, empowering them to make a decision, and moving on that decision. If it's the wrong one, don't be precious about it, you can swap it out for an alternative later. Don't put anything in stone. But fast movement is by far more effective than spending months and months wasting money talking about things that have gone stale before you've even started"*.

Finally, the theme of human resilience is what recursively appears in every article, document or interview referring to Maersk cyber attack, and it was also highlighted in multiple tweets on Maersk official twitter account [see figure 4]. {JHS} stated *"Imagine a company where a ship with 20,000 containers would enter a port every 15 minutes, and for ten days*

you have no IT. It's almost impossible to even imagine. And we actually overcome that problem with human resilience". {GA} highlighted: *"the number of people working around the clock in those early days was staggering. People eating and sleeping in the office. The company booked up every hotel room in the vicinity. People were ferried to and from work in taxis as they were too tired to drive by the end of a shift. Thing is, this went on for weeks and even months for some people. And it affected more than just the people on the ground. This affected careers, families, lives"* [see Figure 4.4].

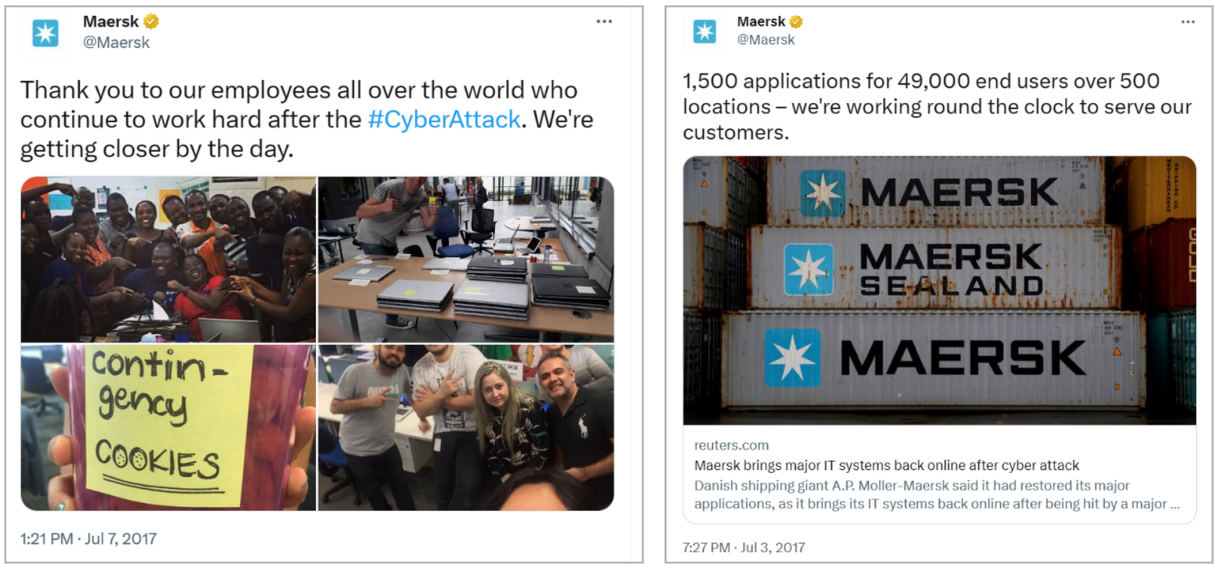


FIGURE 4.4: *Maersk tweets on heroic effort of its employees during the crisis. (Source: Maersk official Twitter account)*

Moreover, {GA} stressed that together with human resilience, also a strong sense of collaboration and team-working allowed employees to effectively carry out their tasks despite the very severe conditions. *"One of the things I'll always cherish about those early days was the tight team dynamic going on. The identity services team all pulled together. Everyone from ops, engineering, architects and managers, partners and vendors. We were all in it. And we broke out into little tactical squads. We cornered a spot in the office and partitioned it off with a giant whiteboard. To get stuff done, we had a rota for people to sit next to the whiteboard to triage any questions or demands coming from the business or other application teams, leaving the rest of team to get on with the task at hand. But there was always respect and only on a couple of occasions did things get heated, which was understandable when the world seemed to be on fire. A real team effort".*

Evidently, despite the initial organizational ignorance and lack of proper communication caused by a general preparedness to face the attack, Maersk was able to optimally respond to NotPetya minimising its potential negative effects thanks to its transparent communication efforts with the external stakeholders, a present and reactive leadership, and a very resilient and committed workforce.

4.4 After the crisis

This period starts about a month after the attack, when Maersk publicly declared it was going back to a normal situation.

Three Third Order Themes have been identified for this stage of the crisis, namely:

1. Organizational learning
2. Organizational implementation
3. Network Leverage

It's worth to notice that the third theme (i.e. Network leverage) was also found in the analysis of the during-crisis stage, as previously described. However, as it will be highlighted later in this section, in this case it has to be understood from a different perspective.

The very first theme that emerged from the analysis was **organizational learning**. After the crisis, Maersk adopted a learning approach that involved a deep investigation of how the company responded to the attack which was aimed at identifying the lessons learned. That attitude allowed the top management to gain a deep understanding of the key error points committed as well as of some good practices that were put in place. Room for improvement was thus identified and corrective actions were implemented.

The major learning can be summarised in the recognition that the threat landscape had completely changed in terms of both threat actors (state-sponsored attackers started entering the scene alongside with the more traditional cybercriminals) and increased vulnerability surface due to the convergence of IT and OT technologies. Consequently, top managers eventually acknowledged the need of a company cultural change with respect to IT and cybersecurity, as well as the need to develop and nurture a new set of skills, tools

and capabilities in order to be able to achieve an optimal cybersecurity posture.

As stated by {JHS} *"[NotPetya] was an important wake-up call. We were basically average when it comes to cyber-security, like many companies. And this was a wake-up call to become not just good — we actually have a plan to come in a situation where our ability to manage cyber-security becomes a competitive advantage"*

Moreover, the golden lessons derived by the cyberattack are clearly outlined by both {AP} and {AG}.

Starting from {AP}, in his speech on implementing the lesson learned from NotPetya attack, he identified multiple golden lessons that were used to guide decisions on how to improve the cybersecurity posture of Maersk. Using his words *"[...] you're having to think in a different way to protect the network. So that attack surface has changed. What we've got to protect against has changed", "It is a golden lesson in itself [learning] about how many of our third party software suppliers represent quite a large risk to us", "another golden lesson.[...] [Offline backup] is the best thing to invest in because a lot of these sorts of high level nation state weapons will take out all your online active directory node", "one of the golden lessons we learnt during the attack was that the IT department used to be those bunch of geeks that nobody talked to, okay? They were just accepted. That is not the case in any business anymore. The joy of being in IT is you are the business. Particularly in digital industries where we're all going, these businesses cannot move forward without us being integrated with them. And that applies to cyber. So when the business folks come up with a new product, you've got to be integrated into that product development from day one", " we learnt which were our critical applications. It's the old classic turn it off. And when the first person squeals, it probably means it's important".*

Furthermore, {AP} also outlined five key principles that were then used as the starting point to build Maersk's cybersecurity strategy *"The most important [principle] is visibility. If you can't see it, you can't fix it. And that's really one of the biggest problems we have. [...] Everybody is responsible for security, okay? That's really important. Not just me. It's not just Andy Powell. It's everybody. And I hold everybody accountable. [...] Third is trust. Build trust with your clients, because we have found that we've got customers flocking back to us to do business with us because they're trust us. There might be the fact that we've been hit once and therefore lightly doesn't strike twice, but I don't think*

that's true. I think they're coming back to us because they see that we put investment into building secure supply chains for them, and that's growing our business by up to 20%. Fourth resilience, as I mentioned earlier, don't just protect, be able to react and recover. And finally, that security is a benefit, not a burden".

To these golden lessons and principles, additional best practices and suggestions were listed by {AG} in his blog: *"Engage with, listen to, and trust, your people. Leaders! Don't rely solely on peers or middle management who may (for completely understandable reasons) try to paint a rosy picture or inadvertently fuzz the details. Get down and dirty. Speak to the folks on the floor, find out what they honestly think. This will build trust up and down the organisation. [...]. Empowerment and agility. Empower people to make decisions and make moves. [...] We saw it in the recovery. If we had to wait that everything was perfect, Maersk wouldn't be here today. [...] Have a plan: Business continuity plans are vital, it's obvious when you say it. But seriously, at whatever level of the organisation you are, there are things you can do to plan for the worst. [..] Plan for that because when it all goes bang, you will seriously thank yourself.[...] Do the basics: [...] doing the basics is straight forward enough. Set the rules, build systems to those rules and gradually migrate legacy systems in or sunset them. But don't waste days, weeks, months or even years failing to act. Don't just talk about it. The fateful day may come at any time".*

Alongside organizational learning, **organizational implementation** was the second major theme playing a key role in the after-crisis period. This concept refers to the ability of the company to translate the lessons learned from the attack, into concrete actions embedded in the organization.

After the crisis, cybersecurity became one of the top priorities for the company. At the top managerial level strategic investments were made to increase the cybersecurity posture of Maersk. A CISO was appointed and he was assigned the task to define and implement a cybersecurity strategy involving people, processes and technologies. Consequently, the required security tools and technologies were implemented, and cybersecurity company-wide frameworks and standards were defined.

Acknowledging that an attack cannot be completely avoided, resulted in the adoption of a proactive security approach, with a perfect balance of protection, reaction, and resilience. Using {AP} words *"For companies like us to try to stop [a cyberattack], it would*

be prohibitively expensive and difficult. So, we have to design measures to recover much more quickly. So, we used nine days to recover from NotPetya attack. In the future now we could do it much, much more quickly. That's because we've designed recovery processes and measures, as well as reactive measures to stop most of the organized crime attacks. [...] And so that's how we've reacted. We've looked at the range of threats and then we built processes around handling that risk." Moreover he stated: *"the real focus is the balance of containment, application vulnerability fix and working on our recovery measures. We now have contingency plans at all our ports and terminals, and you'd be surprised how some of our stevedores who operate in the ports now understand what to do in the event of a cyber crisis. These people have no education, some of them, yet we now train them to deal with a cyber incident should it occur. And they know what to do".*

In addition to that, {AP} also stressed the importance of adopting a risk-based approach to guide investments choices and ensure that the most critical processes to the business were fully protected *"we used a risk based triangle. And at the top of that triangle [we placed] what we call the extinction events to bigger events. And then we worked our way down so that below a certain level in the triangle, systems that only had a localized effect that were damaged, we do stuff about, but we're not investing as much in. That makes sense. But everything at the top of the triangle on those business critical processes that we've got, those five processes that run our company, we have backed those up so we know how we can operate them in the event of those five key processes not working. What I have not done is invest in all the ones below a certain line and it's a risk based approach. You can't back up everything because it would just basically build a second company. [...] So the reality is you've got to have a risk based approach. The risk based triangle is king. And then you've got the hardest bit is to find where you draw the line because it's really hard to get the business to do that".*

Furthermore, to respond to the need of new skills and competencies, after the attack Maersk focused on hiring new talents. Quoting {AP} *" we've bought in a Red Team capability who, if you like, act as our forward lookers. They're looking at the horizon from a Red Team point of view and looking at the emerging threats. [...]They're about 19 in age, and they look young and really young. [...] They wear ripped jeans and nose rings. No offense to those wearing ripped jeans and nose rings. And they talk in a language I don't understand. But they're brilliant because what they're doing is thinking laterally*

and thinking in ways I wouldn't think of. I'm just a guy in a suit. What they're thinking and bringing is original and unique thinking and you've all got to do that. Every big organization needs somebody to do that".

Finally, Maersk's processes were redesigned according to the best practices experienced during the attack. This allowed the company to increase its efficiency and competitiveness. *"We took all those WhatsApp groups that were formed at the time. And we've used that to remodel our business because that was how people worked. They created groups around the way they operated, and we've gone back in and looked at those groups and used that to help rebuild our business processes. [...] some might say it was great we had the attack because it helped us redesign our business. Those WhatsApp groups were formed by many of our younger staff, and they were brilliant because what they were doing was being able to group people together, come up with decisions and work out how to solve problems. Problems were solved in those groups"* {AP}.

The final theme, essential to complete the analysis of Maersk response to the attack, is **network leverage**. In this stage of the crisis, Maersk focused not only on implementing the golden lessons learned from the attack, but also on sharing them with all its external stakeholders. {AP} stated *"one of the golden lessons that I did put up was forensics, forensics, forensics. Every time we currently have a failed cyber attack, I always have a forensics investigation, even if it seems quite small, because every event that you're trying to deal with teaches you something, even if it's quite small. So we will always do a forensics backup. [...] And what we're starting to see, we're sharing. [...] We have to share can I be honest with the folks in this room? We have to share what we know about how these things work openly to stop them".*

Evidently, after the attack Maersk leaders continued to participate to discussion and events to share their experience and suggest best practices on how to approach cybersecurity. Their primary objective was to build a synergic network with customer and suppliers so to increase cybersecurity awareness, which was found to be essential to guarantee the achievement of an optimal cybersecurity posture across the entire value chain.

5 Findings

Following the structure of the reference paper, this section aims to address the research question by linking the Third Order Themes, that arose during the narrative analysis and that were deeply discussed in the previous chapter, to the crisis management leadership competencies defined in the Wooten & James (2008) model.

The findings are summarized in Figure 5.1 and further elaborated in the succeeding sections. Furthermore, the results are compared to the findings of the reference paper so as to confirm or disprove them, as well as to potentially highlight new elements which were not previously considered.

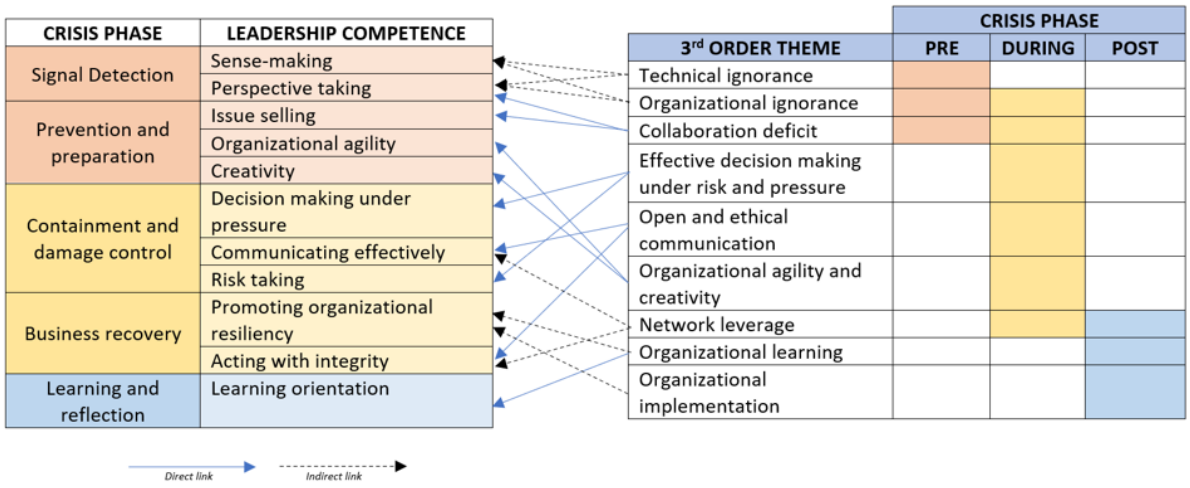


Figure 5.1: *Leadership Competencies and Third Order Themes in Maersk case*

5.1 Signal detection

The first phase to be addressed by the Wooten & James (2008) Model is **signal detection**, in which two leadership competencies are included:

- *Sense-making*: the competence to understand and traduce the present circumstances into an explicit and understandable situation that serves as a reference point for effective decision making;
- *Perspective-taking*: the ability to see things from someone else's viewpoint, a critical element for social interaction and collaboration.

In the Maersk Case, three third order themes can be linked to these competencies. The first two, namely technical ignorance and organizational ignorance, can be linked to both themes, while the third one, collaboration deficit, can be directly linked only to perspective-taking.

Evidently, the company ignorance and lack of awareness about the significance of cybersecurity, resulted in the failure to develop adequate sense-making capabilities that could have allowed Maersk to anticipate the attack or take proactive steps to respond to it as soon as it was experienced. No adequate security tools where in place, no training activities were carried out and no security guidelines, policies, and procedures were defined or followed.

Interestingly, it is worth to notice that while in Wooten & James Model (2008) sense-making

and perspective-taking are related just to signal detection, in Maersk case, the themes of ignorance and collaboration deficit emerged both in the pre-crisis and during-crisis phases of the attack. This highlights that in cyber crisis situations, sense-making is a capability that is necessary not only to early detect the signals of a possible attack, but also to enable quick and timely understanding of its impacts as soon as it takes place. This competence would have allowed Maersk's leaders to avoid the initial state of confusion and paralysis that was experienced in the first moments after being hit by NotPetya ransomware.

As for the lack of sense-making, also the lack of perspective taking was felt both in the pre-crisis, and in the during-crisis phase. Prior to the attack, the poor dialogue between top managers and operative levels of the company resulted in the lack of information sharing, impeding the managerial level to have a deep understanding of the real needs of the company, particularly in terms of safety and security. Moreover, during the first days after the attack, the lack of this competence resulted in Maersk's leaders not to establish a quick interaction with the employees working in Maersk's ports and terminals located far from the main headquarters. They were left in the dark, without any explanation or guideline to follow.

These results constitute further evidence that confirms and extends the reference paper thesis that *"the shortcomings recorded in both competencies [sense-making and perspective taking] highlight the crucial role that cyber-risk aware managers can play in signalling and preventing a cyber-related crisis from happening"*. As for Norsk Hydro's leadership, also Maersk's leadership *"lacked perspective-taking capabilities before the crisis, which [...] led to an important underestimation of the cyber risk to which the company was subjected"* and *"didn't have adequate sense-making capabilities to avoid the attack or respond to it in a proactive manner"*.

In addition, Maersk case demonstrates a further relevant aspect. Cyber-risk aware managers also play a fundamental role in the first moments after the attack takes place. Thanks to the visibility they have of the risks and vulnerabilities of the company, they are able to quickly gain a comprehensive understanding of the situation so to adopt reactive and timely decision making.

5.2 Prevention and preparation

The second phase in the model by Wooten & James (2008) is **prevention and preparation**, in which three leadership competencies are described:

- *Issue-selling*: the competence of employees and middle managers of directing top management's attention to important issues;
- *Organizational agility*: leaders' ability to have a comprehensive understanding of the business processes and units so to be able to get tasks done;
- *Creativity*: the ability to generate out-of-the-ordinary and useful ideas, processes and procedures to achieve given objectives.

As for the analysis of Norsk Hydro, also in the Maersk case, the issue-selling competence is closely linked to the theme of collaboration deficit experienced in the company. Before the attack, Maersk middle managers and IT staff were experiencing great difficulties in communicating to top managers the relevance of the vulnerabilities of Maersk infrastructures and of the consequent alarming risk exposure. This lack of information sharing resulted into an insufficient cyber awareness at all the company levels, eventually causing top managers not to adopt the organizational and technical measures that were needed to ensure prevention and preparation to the attack. This confirms the reference paper finding of *"the crucial need for inter-actor collaboration and transparency to increase an organization's cybersecurity posture"*.

Turning to organizational agility and creativity, both competencies are directly linked to the third order theme organizational agility and creativity, which was fundamental not in the pre-crisis phase, as described in James & Wooten (2008) Model, but during the crisis. This is perfectly in line with the findings of the authors of the reference paper. As in the case of Norsk Hydro, also in Maersk, these two competencies were essential to respond to the attack and guarantee quick recovery minimizing the potential negative impacts of the cyber incident.

In particular, Maersk's leaders showed organizational agility as they were able delegate power to the right people so to ensure that decisions could be made quickly and effectively. Additionally, they proved to be able to foster human resilience and commitment of all the company population, which was the key factor for ensuring containment of the damage

and recovery from the attack. The same applies to creativity. This competence has not to be limited to the prevention and preparation phase, but it must be considered particularly fundamental in the damage containment and business recovery phases as well. In Maersk, the ability to use out-of-the-ordinary solutions was indeed essential to ensure business continuity when the traditional methods were completely disrupted and not usable.

Thus, also Maersk case supports the authors findings that the competencies of organizational agility and creativity *"are found to be useful also and above all during the crisis"*.

5.3 Damage containment

During the third stage, i.e. **damage containment**, Wooten & James (2008) outline three essential capabilities:

- *Decision-making under pressure*: the skill of making quick and sound decisions while under pressure;
- *Risk-taking*: the willingness to take some level of risk while making decision without waiting the availability of perfect information about the situation;
- *Communicating effectively*: the ability to adopt an effective communication strategy to keep the stakeholders informed about the company evolving situation and of the status of the crisis.

In Maersk case, the first two competencies can be found in the third-order theme named effective decision-making under risk and pressure. The analysis of the company response to the crisis highlights that the ability to make quick and effective decisions, to work under pressure, to take risk and to prioritize activities, allowed leaders to achieve quick wins and contain the damage of NotPetya attack.

This finding not only supports the reference paper results, but also extends them. While in Norsk Hydro, *"it was not possible to trace a precise connection between 3rd-order theme and the risk-taking capability"*, in Maersk case, leaders' competence of making decisions under uncertainty without waiting everything was perfectly clear, resulted to be vital to avoid paralysis and respond to the attack.

As for the competence of communicating effectively, this can be linked to the theme open and effective communication. Like Norsk Hydro's leaders, also Maersk's top management adopted since the beginning a consistent, open and transparent communication plan to keep all the stakeholders informed about the company status. This allowed Maersk to maintain strong relationships with its customers and suppliers which continued to trust and remain loyal to the company also in the most critical situations. Evidently this helped Maersk to minimize the potential losses of the attack.

Furthermore, also the theme of network leverage is indirectly related to the competence of effective communication. Differently from the reference paper, where this specific theme is not discussed, in Maersk case, effective communication also helped the company to build a strong network with its customers, suppliers and partners. This network turned out to be essential during the crisis because it allowed to share skills, competencies, and technologies that Maersk was lacking, and that where fundamental to respond to the attack. Furthermore, as it will be detailed in the next paragraphs, the nurturing of such network proved to be important also to foster resilience after the attack since it was used as a channel to share lesson learned and increase cybersecurity awareness across all the company value chain.

5.4 Business recovery

Wooten and James (2008) identify two competencies for the fourth stage of **business recovery**:

- *Promoting organizational resiliency*: the ability to return the organization to its pre-crisis state;
- *Acting with integrity*: the ability to engage in ethical decision making and behaviours.

Starting from the first competence, promoting organizational resiliency can be linked to both organizational learning and organizational implementation themes. Maersk's leaders approached the crisis as a catalyst to think differently about the organization to make it better off than as it was before. Processes were re-designed, new talents were hired and new skills and competencies were developed and trained. Evidently a resiliency approach was used so to make the company more robust and ready to face future adversities.

This confirms the findings of the reference paper's authors that *"moving towards resilience is something that can be indirectly connected to the themes of organizational learning and organizational implementation"*.

As for the competence of acting with integrity, this is directly linked with the theme of open and ethical communication, and indirectly connected also to the theme of network leverage.

Similarly to what was found in Norsk Hydro Case in which the authors noted that *"Wooten & James mention this competence among the ones relevant after the crisis, while from the narrative analysis it emerges that it was actually fundamental since its beginning"*, also in Maersk case the leaders ability to engage in ethical and consistent communication with all the stakeholders involved, was vital in the response to the attack starting from the very first moments. Acting with integrity was indeed essential both during the crisis, in which it was key to maintain the trust of the diverse stakeholders involved, and after the crisis, where it was essential to involve them in the learning activities.

5.5 Learning and reflection

For the last stage, **learning and reflection**, Wooten and James (2008) identify only one competence:

- *Learning orientation*: the ability to put in place post-crisis learning activities to enhance recovery capabilities.

This competence aligns with the third order theme of organizational learning, perfectly supporting what was found by the reference paper. As for Norks Hydro, in which *"The key learnings appearing from the analysis are 1) the increased need for organizational cyber awareness and 2) the need for an organizational cybersecurity and cyber resilience strategy"*, also in the case of Maersk the main golden lessons were the need of a culture change so as to recognise cybersecurity and cyber awareness as a competitive advantage, and the needed to develop new skills, tools and capacities to enhance the cybersecurity posture of the company. These learnings were at the base of all the company activities performed after the crisis.

Interestingly, similarly to Norsk Hydro, also in the analysis of Maersk the theme of organizational implementation emerges, but it cannot be directly linked to any leadership competence identified by Wooten and James (2008). The authors of the reference paper argue that this theme *"is not a synonym of the organization learning, but rather its natural complement. In fact, this is a fundamental activity for the company, and actually the one that led Norsk Hydro to become more resilient to cyber risk in the following two years"*. This statement is fully supported by the findings of the analysis of Maersk. Its leaders' ability to transform the lesson learned into concrete actions allowed the company not only to learn from the attack, but also to turn these learnings into opportunities to develop new processes, behaviours and activities that ultimately contributed to change the way the company operated.

6 Conclusions

In the recent years, the proliferation of digital technologies has resulted in a corresponding surge in both the quantity and severity of cybercrimes, with ransomware attacks playing a significant role in this trend. Despite the consequent increase of cyber-related organizational crises and the growing recognition of their threat to society, there is a notable lack of academic literature on how companies can effectively develop crisis management processes and capabilities in this area, particularly with regards to leadership competencies.

The reference paper, *Understanding the Role of Leadership Competencies in Cyber Crisis Management: A Case Study*, (Salviotti et al., 2023) presented at the 56th Hawaii International Conference on System Science 2023, starts to address this gap by evaluating the effectiveness of traditional crisis management leadership competencies in the context of cyber crises. By employing the Wooten & James (2008) model in the context of the Norsk Hydro case, the study outlines valuable insights and it highlights the traditional leadership competencies that turned out to be most effective in dealing with a cyber crisis.

Through the analysis of the Maersk case, this thesis further extends the research started by the authors of the reference paper. In particular, by using the same analysis methodology, the investigation of the selected case study has produced findings that not only confirm

the results of the reference paper, but also reveal new elements which were not previously considered.

In particular, from the analysis of Maersk case, the very same major issue highlighted by the reference paper emerges: *"cyber-related crises are strictly connected with a poor managerial ability to foresee the implications of cyber risk and consequently coordinate the necessary prevention and preparation actions. In practical terms, this implies the need for an increased level of cyber awareness at both the top and middle management levels"*.

The analysis further supports the relevance of issue-selling competence, which is at the base of an effective collaboration among different levels of the company and thus it is pivotal to guarantee a strong cybersecurity posture of the organization. In addition, Maersk case demonstrates that cyber-risk aware managers also play a fundamental role not only to prevent the crisis, but also to timely respond to the attack if it is eventually experienced. In this scenario, thanks to the visibility cyber-risk aware managers have of the risks and vulnerabilities of the company, they are able to avoid paralysis and adopt reactive and timely decision making.

During the crisis, the competencies that the study demonstrates to play a major role in facing the attack are effective communication and the ability to make decisions under risk and pressure, as described by the Wooten & James (2008) model. This also confirms the reference paper findings that *"communication efforts should be as much open and transparent as possible, and addressed both internally and externally to maintain a high level of trust with employees, partners, providers and customers"*.

Maersk case highlights an additional competence that did not emerge in the reference paper and which was not included in the Wooten & James (2008) model, namely the ability to develop and nurture a strong network with customers, suppliers and partners in order to share skills, competencies, technologies and learnings. This is fundamental in the field of cybersecurity where, due to its high interconnected and interdependent nature, a strong and synergic collaboration among different actors is needed to achieve a strong cybersecurity posture.

Furthermore, the thesis supports what Norsk Hydro case revealed in terms of the role of creativity and organizational agility, which again were found to be two competencies

that *"can be useful not only in the prevention phase, but also and above all during the crisis. The former can prove very helpful to figure out how an organization can operate without having access to its normal systems, thus strengthening the company's continuity capability. The latter, in conjunction with a strong organizational culture, can accelerate and facilitate crisis-overcoming efforts"*.

Also *"the importance of acting with integrity within the cyber crisis scenario, postulating that openness and transparency in the response to the crisis can have an even wider effect if followed from the beginning of the crisis"* is further confirmed by the analysis of Maersk case in which the ethical behaviour adopted by the leaders was essential to maintain trust, loyalty and commitment both of the internal and of the external stakeholders.

To conclude, dealing with the post-crisis phase, this thesis strongly supports the reference paper claim that one of the most important post-crisis leadership competencies is the implementation of the learnings from the crisis, which is not considered in the Wooten & James (2008) model. Maersk case indeed is a further proof that *"organizational implementation is the step that can effectively lead to the creation of a cyber-resilient security culture that acts proactively and not reactively"*.

Given the rapid progression of cybercrimes and their severe impacts on both organizations and society, it is imperative to enhance our understanding of cyber-related crises. Therefore, examining this topic is both essential and pressing. By extending the previous results, this thesis increases the current body of knowledge on how organizations can effectively handle cyber-related crises, thus facilitating their advancement towards cyber resilience and providing valuable insights which can be used to create models and reference frameworks in the field of cyber crisis management.

6.1 Managerial Implications and Future Work

By comparing and integrating the results obtained from the investigation of the two major cyber crises experienced by Maersk and Norsk Hydro, this thesis offers very valuable managerial implications that can guide leaders in reinforcing their company's cybersecurity posture and acquiring the necessary tools, skills, and competencies to effectively navigate through a cyber crisis.

Overall, the thesis highlights the need for a comprehensive and proactive cybersecurity posture that integrates protection, reaction, and recovery aspects. Indeed, the ever evolving and increasingly complex threat landscape, makes it impossible for companies to completely zero the risk of being hit by a cyberattack. Thus it is vital to allocate investments and resources not only to protect the organization, but also to strengthen its ability to respond in case a cyber crisis eventually occurs.

The development of a cybersecurity strategy that is aligned with the business and digital strategies, as well as the identification of core functions, vulnerabilities, and threat actors, is essential for a company to prioritize actions and allocate resources effectively. This requires top managers to start perceiving cybersecurity as a business enabler rather than a cost to be minimised.

Cybersecurity investments should follow a risk based approach which requires leaders to gain full visibility of both the internal and external context in which the company operates. This will allow them to define security policies and guidelines specifically tailored to the company's needs. Once defined, those procedures need to be embedded in the company's operations so that all its employees, regardless of their profile and positions, follow them during their daily activities.

Furthermore, it is also vital to plan and prepare for a possible crisis. It is important to define a business continuity and recovery plan which should be continuously exercised and maintained. Training, awareness, and education programs should be developed to equip employees with the necessary skills and competencies to respond to a cyber attack. Education activities should also target the development of lateral and soft skills (team working, creativity and decision making under risk and time pressure) which can be the differentiating factor during a crisis.

Company culture and values should be also given particular attention by top managers as they play a vital role in promoting inter-actor collaboration, employee commitment, and information sharing, which are essential elements to increase the security posture of the company.

During a crisis, transparent and open communication, present and reactive leadership, as well as network leverage, are critical factors to ensure an effective response. The

involvement of leaders in all crisis-related activities, and the creation of a network with external stakeholders are essential to maintain the company's agility and responsiveness during the crisis, and to increase the cybersecurity posture and resilience of the entire value chain in its aftermath.

Based on this initial analysis and recommendations, future work could focus on further refining the concepts covered in a more structured manner with the final objective to develop a reference model that can guide companies' top managers in building the skills and competencies needed to deal optimally with a cyber crisis.

The development of such reference model would be particularly relevant for public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934, as it would help them to comply with the new rules proposed by the Securities and Exchange Commission (SEC) in 2022 regarding cybersecurity risk management, strategy, governance, and incident disclosure practices (U.S. Securities and Exchange Commission, 2022).

Recognising that cybersecurity crises can greatly impact the financial performance of a company, and consequently also investors' return on investments, SEC has proposed new rules that require public companies to periodically disclose consistent, comparable, and decision-useful information regarding their cybersecurity risk management, strategy, and governance practices, as well as a their response to material cybersecurity incidents, and their management and board of directors' oversight role and cybersecurity expertise.

The final objective of this proposal is to allow investors to better evaluate a company's risk management and governance practices, so to better inform their investments and voting decisions.

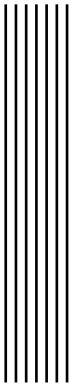
6.2 Limitations

This thesis addresses one of the main limitations presented by the reference paper in which the authors called for *"further research [that] could investigate other case studies that display other characteristics (different geography, response, etc.)"*. By analysing a new case study, this thesis allowed to take the perspective of a company different in

terms of size, geography and business model, thus broadening the scope of investigation. Consequently, the alignment of the findings of the two different cases is a proof of their relevance, goodness and validity.

However, as for the reference paper, also in this thesis the primary limitation derives from the data collection, which relies only on secondary qualitative data. Thus, future research, as already suggested by the authors of the reference paper, could benefit from a more depth exploration of the present case study, gathering primary data directly from the stakeholders involved in the attack which could reveal further insights in Maersk's top management leadership style and crisis management strategies.

To conclude, even though this case confirms and extends the previous findings, this research area is still insufficiently explored and further analysis is needed to build and consolidate more knowledge in the field of leadership competencies in cyber crisis management.



Bibliography

C. Ansell and A. Keller. Managing transboundary crises: Identifying the building blocks of an effective response system. *Journal of Contingencies and Crisis Management*, 18 (4), 2010. URL https://doi.org/10.1111/j.1468-5973.2010.00620.x.

G. Ashton. Maersk, me & notpetya (personal blog). URL https://gvnshtn.com/posts/maersk-me-notpetya/. Accessed: 2023.04.22.

S. Backman. Conceptualizing cyber crises. *Journal of Contingencies and Crisis Management*, 29(4):0966–0879, 2020. URL https://doi.org/10.1111/1468-5973.12347.

Bank Infosecurity series - The Ransomware Files (podcast). Episode 4: Maersk and notpetya, malware disguised as ransomware nearly sank logistics giant maersk, 25 January 2022. URL https://www.bankinfosecurity.com/interviews/ransomware-files-episode-4-maersk-notpetya-i-5014. Accessed: 2023.04.22.

J. M. Bartunek. Changing interpretive schemes and organizational restructuring: The example of a religious order. *Administrative Science Quarterly*, 29(3):355–372, 1984. URL http://www.jstor.org/stable/2393029.

M. Benali and A. R. Ghomari. Information and knowledge driven collaborative crisis management: A literature review. In *2016 3rd International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*, pages 1–3, 2016. URL https://doi.org/10.1109/ICT-DM.2016.7857229.

Black Hat Europe (Youtube Video). Implementing the lessons learned from a major cyber attack, 2-5 December 2019. URL https://youtu.be/wQ8HIjkEe9o. Accessed: 2023.04.22.

A. R. Boin and M. M. Ekengren. *Handbook of Security and Governance*, chapter Transboundary Crisis Governance, pages 307–323. Cheltenham: Edward Elgar, 2014.

L. C. Bolman and T. E. Deal. *Refraining organizations*. San Francisco: Jossey-Bass, 1997.

A. Bonime Blanc. Cyber organizational resilience is a business imperative: the essential eight steps to get there. In *Actuarios: Ciberriesgos*, volume 48, pages 33–41, 2021.

D. Braue. Global ransomware damage costs predicted to exceed $265 billion by 2031, 2022. URL https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/. Accessed: 2023.04.22.

J. Bundy, M. D. Pfarrer, C. E. Short, and W. T. Coombs. Crises and crisis management: Integration, interpretation, and research development. *Journal of Management*, 43(6): 1661–1692, 2017. URL https://doi.org/10.1177/0149206316680030.

J. Burnett. *Managing business crises: From anticipation to implementation*. Westport, CT: Quorum Books, 2002.

M. Butina. A narrative approach to qualitative inquiry. *American Society for Clinical Laboratory Science*, 28(3):190–196, 2015. URL https://doi.org/10.29074/ascls.28.3.190.

Cambridge University Center for Risk Studies and RMS. Cyber risk outlook, 2019. URL https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/technology-and-space/cyber-risk-outlook/cyber-risk-outlook-2019/. Accessed: 2023.04.22.

D. E. Capano. Throwback attack: How notpetya accidentally took down global shipping giant maersk, 2021.

CISA Cybersecurity Advisory. Trends show increased globalized threat of ransomware, 2022. URL https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-040a. Accessed: 2023.04.22.

D. J. Clandinin and F. M. Connelly. *Narrative inquiry: Experience and story in qualitative research*. Jossey-Bass, 2000.

W. Coombs and S. Holladay. An extended examination of the crisis situations: A fusion of the relational management and symbolic approaches. *Journal of Public Relations Research - J PUBLIC RELAT RES*, 13:321–340, 10 2001. URL https://doi.org/10.1207/S1532754XJPRR1304_03.

W. T. Coombs. *Ongoing Crisis Communication. Planning, Managing, and Responding. SIXTH EDITION.* SAGE Publications, Inc, 2022.

Darknetdiaries (podcast). Episode54: Notpetya. URL https://darknetdiaries.com/transcript/54/. Accessed: 2023.04.22.

G. V. der Loo. *The EU-Ukraine Association Agreement and Deep and Comprehensive Free Trade Area: A New Legal Instrument for EU Integration without Membership.* (Leiden, Belgium: Brill Nijhoff, 2016.

S. Duchek. Organizational resilience: a capability-based conceptualization. *Business Research*, 13:215–246, 2020. URL https://doi.org/10.1007/s40685-019-0085-7.

K. M. Eisenhardt. Building theories from case study research. *The Academy of Management Review*, 14(4):532–550, 1989. URL https://doi.org/10.2307/258557.

ENISA. Enisa threat landscape for ransomware attacks, 2022a.

ENISA. Enisa threat landscape 2022, 2022b.

S. Y. A. Fayi. *Information Technology - New Generations*, chapter What Petya/NotPetya Ransomware Is and What Its Remidiations Are, pages 93–100. Springer Link, 2018. URL https://doi.org/10.1007/978-3-319-77028-4_15.

Federal Bureau of Investigation. Internet Crime Compliant Center. Internet crime report, 2021. URL https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf. Accessed: 2023.04.22.

Financial Times. Maersk ceo soren skou on surviving a cyber attack, 13 August 2017. URL https://www.ft.com/content/785711bc-7c1b-11e7-9108-edda0bcbc928. Accessed: 2023.04.22.

S. Fink. *Crisis management: Planning for the inevitable.* New York, NY: AMACOM, 1986.

S. L. Fink, J. Beak, and K. Taddeo. Organizational crisis and change. *The Journal of Applied Behavioral Science*, 7(1):15–37, 1971. URL https://doi.org/10.1177/002188637100700103.

U. Flick. *An introduction to qualitative research.* Sage Publications, 2018.

Y. Gabriel. *Storytelling in organizations: Facts, fictions, and fantasies.* Oxford University Press, 2000.

H. Garcia. Effective leadership response to crisis. *Strategy and Leadership*, 34(1):4–10, 2006.

C. Glesne. *Becoming Qualitative Researchers: An Introduction.* Boston, MA: Pearson Education, Inc, 2006.

Y. Golandsky. Cyber crisis management, survival or extinction? In *2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*, pages 1–4, 2016. URL https://doi.org/10.1109/CyberSA.2016.7503291.

A. Greenberg. The untold story of notpetya, the most devastating cyberattack in history. *Wired*, 24 August 2018. URL www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/. Accessed: 2023.04.22.

D. Guth. Organizational crisis experiences and public relations roles. *Public Relations Review*, 21, 06 1995. doi: https://doi.org/10.1016/0363-8111(95)90003-9.

C. Hu, K. H. Yun, Z. Su, and C. Xi. Effective crisis management during adversity: Organizing resilience capabilities of firms and sustainable performance during covid-19. *Sustainability*, 14(20):13664, 2022. URL https://doi.org/10.3390/su142013664.

IBM. Cost of a data breach report, 2022. URL https://www.ibm.com/downloads/cas/3R8N1DZJ. Accessed: 2023.04.22.

Infosecurity Europe (youtube video). Maersk 's ctio adam banks about notpetya ransomware attack, 2019. URL https://www.youtube.com/watch?v=_MwsxIS3tG8. Accessed: 2023.04.22.

E. James, L. Wooten, and K. Dushek. Crisis management: Informing a new leadership research agenda. *The Academy of Management Annals*, 5:455–493, 06 2011. URL https://doi.org/10.1080/19416520.2011.589594.

E. H. James and L. P. Wooten. (un)usual: How to display competence in times of crisis. *Organizational Dynamics*, 34(2):141–152, 2005. URL https://doi.org/10.1016/j.orgdyn.2005.03.005.

M. Langan-Riekhof, A. B. Avanni, and A. Janetti. Sometimes the world needs a crisis: Turn-

ing challenges into opportunities, 2017. URL https://www.brookings.edu/research/sometimes-the-world-needs-a-crisis-turning-challenges-into-opportunities/. Accessed: 2023-04-22.

B. A. Loewendick. Effective leadership response to crisis. *Training & Development*, 47 (11):15–17, 1993.

K. Lowe. *Savage Continent: Europe in the Aftermath of World War II*. New York: Picador, 2013.

Maersk. Cyber attack update, 18 June 2017. URL https://investor.maersk.com/news-releases/news-release-details/cyber-attack-update. Accessed: 2023.04.22.

Maersk Annual Reports. Annual reports from 2016 to 2021. URL https://investor.maersk.com/financials/financial-reports. Accessed: 2023.04.22.

Maersk Company Website. The history and heritage of a.p. moller - maersk. URL https://www.maersk.com/about/our-history/explore-our-history. Accessed: 2023.04.22.

P. R. Magocsi. *A History of Ukraine: The Land and Its People*. Toronto: University of Toronto Press, 2012.

V. H. Mair. "crisis" does not equal "danger" plus opportunity". how a misunderstanding about chinese characters has led many astray, 2009. URL http://pinyin.info/chinese/crisis.html. Accessed: 2023-04-22.

T. McIntosh, A. S. M. Kayes, Y.-P. Chen, A. Ng, and P. Watters. Ransomware mitigation in the modern era: A comprehensive review, research challenges, and future directions. *ACM Computing Surveys*, 54:1–36, 10 2021. URL https://doi.org/10.1145/3479393.

M. E. Menshawy. Notpetya tactical report, 2019. URL https://menshaway.blogspot.com/2019/07/notpetya-tactical-report.html. Accessed: 2023.04.22.

T. H. Mitchell. Coping with a corporate crisis. *Canadian Business Review*, 13:17–20, 1986. doi: https://doi.org/10.1016/0363-8111(95)90003-9.

I. Mitroff and M. Alpaslan. Preparing for evil. *Harvard Business Review*, 81(4):109–115, 2003.

I. I. Mitroff. Crisis management and environmentalism: A natural fit. *California Management Review*, 36(2):101–113, 1994. URL https://doi.org/10.2307/41165747.

I. I. Mitroff and C. M. Pearson. *Crisis Management: A Diagnostic Guide for Improving Your Organization's Crisis-Preparedness.* San Francisco: Jossey-Bass, 1993.

NCSC National Cyber Security Center. Russian military 'almost certainly' responsible for destructive 2017 cyber attack, February 2017.

L. H. Newman. The leaked nsa spy tool that hacked the world, 7 March 2018. URL `www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/`. Accessed: 2023.04.22.

NIST Glossary. Definition of malware. URL `https://csrc.nist.gov/glossary/term/malware`. Accessed: 2023.04.22.

OBR Office for Budget Responsibility. Cyber-attacks during the russian invasion of ukraine, July 2022. URL `https://obr.uk/box/cyber-attacks-during-the-russian-invasion-of-ukraine/`. Accessed: 2023.04.22.

Papers of John F. Kennedy. Pre-Presidential Papers. Senate Files, Box 902, "United Negro College Fund, Indianapolis, Indiana, 12 April 1959." John F. Kennedy Presidential Library. 12 April 1959. URL `https://www.jfklibrary.org/asset-viewer/archives/JFKSEN/0902/JFKSEN-0902-023`. Accessed: 2023-04-22.

A. Paraskevas. Crisis management or crisis response system? a complexity science approach to organizational crises. *Management Decision*, 44(7):892–907, 2006. URL `https://doi.org/10.1108/00251740610680587`.

C. M. Pearson and J. A. Clair. Reframing crisis management. *The Academy of Management Review*, 23(1):59–76, 1998. URL `https://doi.org/10.2307/25909`.

C. M. Pearson and I. I. Mitroff. From crisis prone to crisis prepared: A framework for crisis management. *The Executive*, 7(1):48–59, 1993. URL `http://www.jstor.org/stable/4165107`.

R. Perry and E. L. Quarantelli. *What Is a Disaster? New Answers to Old Questions.* Xlibris Books, 2005.

D. E. Polkinghorne. Narrative configuration in qualitative analysis. *International Journal of Qualitative Studies in Education*, 8(1):5–23, 1995. URL `https://doi.org/10.1080/0951839950080103`.

V. Potocan and Z. Nedelko. The behavior of organization in economic crisis: Integration,

interpretation, and research development. *J Bus Ethics*, 174:805–823, 2021. URL https://doi.org/10.1007/s10551-021-04928-8.

Predica. Conquering notpetya: Two weeks on the front line, 15 June 2018. URL https://predica.pl/blog/conquering-notpetya/. Accessed: 2023.04.22.

M. Prevezianou. Beyond ones and zeros: Conceptualizing cyber crises. *Risk, Hazards & Crisis in Public Policy*, 12, 12 2020. doi: https://doi.org/10.1002/rhc3.12204.

Pwc and Oxford-Metrica. Corporate reputation in crisis: The impact on shareholder value, 2020.

C. K. Riessman. *Narrative methods for the human sciences*. Sage, 2008.

J. Roessler. *Can Annexation Be Justified? Analysing Russia's Annexation of Crimea*. Munich: GRIN Publishing, 2017.

U. Rosenthal. September 11: Public administration and the study of crises and crisis management. *Administration & Society*, 35(2):129–143, 2003. URL https://doi.org/10.1177/0095399703035002001.

U. Rosenthal, M. T. Charles, and P. 't. Hart. *Coping with Crises: The Management of Disasters, Riots and Terrorism*. C.C. Thomas, Springfield, Ill., U.S.A., 1989.

M. Ryan. *Ransomware Revolution: The Rise of a Prodigious Cyber Threat*. Springer Link, 2021.

S. Sahin, S. Ulubeyli, , and A. Kazaza. Innovative crisis management in construction: Approaches and the process. *Procedia – Social and Behavioral Sciences*, 195:2298–230, 2015. URL https://doi.org/10.1016/j.sbspro.2015.06.181.

G. Salviotti, N. Abbatemarco, L. M. De Rossi, and K. Bjoernland. Understanding the role of leadership competencies in cyber crisis management: A case study. In *Proceedings of the 56th Hawaii International Conference on System Sciences*, pages 6068–6078, 2023. URL https://hdl.handle.net/10125/103370.

SE-RADIO (podcast). Episode 438: Andy powell on lessons learned from a major cyber attack, 12 December 2020. URL https://www.se-radio.net/2020/12/episode-438-andy-powell-on-lessons-learned-from-a-major-cyber-attack/. Accessed: 2023.04.22.

P. Shrivastava. Crisis theory/practice: towards a sustainable future. *Industrial & Environmental Crisis Quarterly*, 7(1):23–42, 1993. URL https://doi.org/10.1177/

108602669300700103.

K. Sood and S. Hurley. Notpetya technical analysis – a triple threat: File encryption, mft encryption, credential theft, 29 June 2017. CrowdStrike (blog).

SOPHOS. The state of ransomware, 2022. URL https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf. Accessed: 2023.04.22.

R. E. Stake. *The art of case study research.* Sage, 1995.

A. L. Strauss. Qualitative analysis for social scientists. *Cambridge University Press*, 1987. URL https://doi.org/10.1017/CBO9780511557842.

D. Swinhoe and Editor, CSO. Rebuilding after notpetya: How maersk moved forward, 9 October 2019. URL https://www.csoonline.com/article/3444620/rebuilding-after-notpetya-how-maersk-moved-forward.html. Accessed: 2023.04.22.

The White House. Statement from the press secretary, 15 February 2018.

U.S. Securities and Exchange Commission. Proposed rules on cybersecurity risk management, strategy, governance, and incident disclosure by public companies. 9 March 2022. URL https://www.sec.gov/news/press-release/2022-39.

G. S. van der Vegt, P. Essens, M. Wahlström, and G. George. Managing risk and resilience. *Academy of Management Annals*, 58(4):971–980, 2015. URL https://doi.org/10.5465/amj.2015.4004.

Verizon. Data breach investigations report, 2022. URL https://www.verizon.com/business/resources/reports/dbir/. Accessed: 2023.04.22.

M. V. Wart and N. Kapucu. Crisis management competencies. *Public Management Review*, 13(4):489–511, 2011. URL https://doi.org/10.1080/14719037.2010.525034.

P. J. J. Welfens and E. Gavrilenkov. *Restructuring, Stabilizing and Modernizing the New Russia: Economic and Institutional Issues.* Berlin: Springer, 2000.

D. T. Wesley, L. A. Dau, and A. Roth. Unpack the case: Cyberattack: The maersk global supply-chain meltdown, September 2019.

M. Williams and T. Moser. The art of coding and thematic exploration in qualitative research. *International Management Review*, 15:45, 2019.

T. A. Williams, D. A. Gruber, K. M. Sutcliffe, D. A. Shepherd, and E. Y. Zhao. Organizational response to adversity: Fusing crisis management and resilience research streams. *Academy of Management Annals*, 11(2):733–769, 2017. URL https://doi.org/10.5465/annals.2015.0134.

L. P. Wooten and E. H. James. Linking crisis management and leadership competencies: The role of human resource development. *Advances in Developing Human Resources*, 10 (3):352–379, 2008. URL https://doi.org/10.1177/1523422308316450.

World Economic Forum. Securing the future of cyberspace. youtube video, 59:06, 24 January 2018. URL www.youtube.com/watch?time_continue=224&v=Tqe3K3D7TnI. Accessed: 2023.04.22.

World Economic Forum. The global risks report 2022, 17th edition, 2022.

World Economic Forum. The global risks report 2023, 18th edition, 2023.

R. Yin. *Case Study Research: Design and Methods (5th ed.)*. Thousand Oaks, CA: Sage Publications, Inc, 2014.