Understanding Leadership Competencies in Cyber Crisis Management: Insights from the Maersk Global Supply Chain Meltdown

Nico Abbatemarco
SDA Bocconi School of Management
nico.abbatemarco@sdabocconi.it

Gianluca Salviotti
SDA Bocconi School of Management
gianluca.salviotti@sdabocconi.it

Leonardo De Rossi
SDA Bocconi School of Management
leonardo.derossi@sdabocconi.it

Chiara D'Ignazio
Università Bocconi
chiara.dignazio@studbocconi.it

Abstract

In today's rapidly evolving digital landscape, organizations face an increasing threat from cyber-attacks and the resulting cyber crises. This paper focuses on the management of such crises, specifically examining the case study of the NotPetya cyber-attack that hit Maersk, a global shipping company, in 2017. Through the analysis of qualitative data and utilizing a Narrative Inquiry approach, this study aims to deepen the understanding of the leadership competencies required to effectively navigate and mitigate the impact of cyber crises. By emphasizing competencies such as sense-making, perspective-taking, and risk-taking in the immediate aftermath of an attack, this paper contributes to the growing body of knowledge in the field of cyber crisis management. Additionally, the paper highlights the crucial role played by leaders in leveraging the organization's external network to establish end-to-end cyber resilience across the supply chain.

Keywords: Cybersecurity, Cyber Risk, Cyber Crisis, Crisis Management, Leadership Competencies.

1. Introduction

In today's interconnected world, societies are confronted with a diverse range of crises that pose significant challenges to their stability and well-being. The World Economic Forum's (WEF) Global Risk Perception Survey 2022-2023 identified several risks that have the potential to impact the global landscape profoundly, from "Energy supply crises" to "Cyberattacks on critical infrastructure" (WEF, 2023).

In this scenario, it becomes imperative for organizations of all types to be prepared to face crises. Consequently, investing resources in the adoption and development of crisis management measures, tools, and core competencies is more crucial than ever. 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 (Liu et al., 2017; Pearson & Clair, 1998; Robert & Lajtha, 2002). Following a crisis, organizations can be divided into two distinct groups: "winners", who recover successfully and ultimately increase their value, and "losers", who suffer prolonged negative effects (Bibeault, 1998; Boin et al., 2013). Leadership competencies can play an especially important role in turning losers into winners – and vice versa (Boin et al., 2013; Wooten & James, 2008).

While traditional crises pertaining to societal and economic domains have long been acknowledged, the rapid pace of technological advancements and their integration into critical societal functions have brought forth new and complex cyber-related ones. The WEF 2023 report specifically emphasizes the escalation of malicious activities in cyberspace, characterized by increasingly aggressive and sophisticated cyberattacks taking advantage of a widespread attack surface. Given the increasing frequency and severity of cybercrimes on a global scale, it is reasonable to assume that identifying specific factors that can help organizations in navigating cyber crises would provide valuable insights to both researchers and practitioners. However, the academic literature on this topic is quite lacking. Many scholars tried to conduct a conceptual analysis of cyber crises and questioned whether the vast knowledge gained in the traditional crisis domain remains still relevant in this new field (Backman, 2021; Golandsky, 2016; Prevezianou, 2021). Their research highlighted the presence of a still wide gap in this sense, which "calls for academic exploration of this terra incognita" (Prevezianou, 2021, p.56).

One of the first papers that started to fill this gap was Salviotti et al. (2023), which aimed at understanding how and to what extent leadership

URI: https://hdl.handle.net/10125/106892
978-0-9981331-7-1

competencies contribute to mitigate the negative impacts of a cyber crisis. While its findings provide initial insights into understanding which are the relevant capabilities required to successfully handle cyber crises, the same authors pointed out that further investigation is required to confirm the validity of their findings and eventually reveal additional evidence.

Therefore, this paper builds upon Salviotti et al. (2023) with the aim of further contributing to the field of cyber crisis management, by expanding the understanding of effective leadership competencies in cyber crises. By analyzing a different case study, namely the Maersk Global Supply Chain Meltdown, this research aims to validate or challenge the findings of the reference paper and uncover new ones.

The paper is organized into five sections. Section 2 provides a comprehensive theoretical background for the topic at stake. Section 3 outlines the methodology employed, including the selection of the case study and the data collection procedure. Section 4 delves into the analysis of the selected case study, offering insights into how the cyber crisis was managed. Section 5 discusses the findings and compares them to the reference paper's results. Finally, Section 6 serves as a conclusion, summarizing the work, evaluating its contributions, and suggesting avenues for future research.

2. Literature review

This section provides a comprehensive theoretical background that encompasses crisis and crisis management, crisis leadership competencies and then contextualizes them in relation to cyber crises. It also highlights the challenges and gaps in the cyber crisis field and presents the reference paper's main findings.

2.1 Crisis and crisis management

A unique and widely accepted definition of crisis or crisis management remains elusive due to the interdisciplinary nature of the field (Coombs, 2023). To address this issue, we refer to the definitions of crisis and crisis management provided by Pearson & Clair (1998). Pearson & Clair (1998) tried to frame a comprehensive definition that integrated various viewpoints in the field. According to their definition (p.60), "a 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". On the other hand, they defined crisis management (p.66) as the set of activities aimed at "minimizing potential risk before a triggering event" and that in response to such event involves improvising and interacting with key stakeholders so that individuals and collective sense making, shared meaning, and roles are reconstructed".

Several scholars have investigated how crisis management is essential for an organization's sustainable performance and survival (Duchek, 2020; Van Der Vegt et al., 2015; Williams et al., 2017). Therefore, several approaches have been developed to study crisis management and help companies develop response plans and strategies.

Table 1. Comparison of approaches to crisis management (Source: Coombs, 2023).

Fink	Mitroff	Three-stage
1. Prodromal	1. Signal Detection 2. Prevention and Preparation	1. Pre-crisis
2. Crisis breakout 3. Chronic	3. Damage Containment 4. Recovery	2. Crisis
4. Resolution	5. Learning	3. Post-crisis

Among these, Fink's approach (Fink, 1986), Mitroff's model (Mitroff, 1994), and the three-stage model (used for example by Coombs & Holladay, 2001) have been recognized as the most influential (Coombs, 2023) (see Table 1).

2.2 Crisis management and leadership competencies

Research has shown that leadership competencies are crucial in determining whether an organization will emerge with a positive or negative impact after a crisis (Bundy et al., 2017; James et al., 2011; Van Wart & Kapucu, 2011; Wooten & James, 2008). The role of organizational leaders and the impact of their decisions are magnified during times of crisis, and can have a major impact on the effectiveness of crisis management (Coombs, 2023; Van Wart & Kapucu, 2011).

Table 2. Leadership competencies in crisis management (adapted from Wooten & James, 2008)

Crisis phase	Competencies
Signal detection	Sense-making
	Perspective-taking
Prevention and preparation	Issue-selling
	Using creativity
	Fostering org. agility
Damage containment	Communicating effectively
	Decision-making
	Risk-taking
Business recovery	Acting with integrity
	Promoting resilience
Learning and reflection	Fostering learning orientation

Given the importance of this subject, Wooten & James (2008) 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 summarized in Table 2. The leadership competencies addressed by the Wooten & James (2008) model are eleven, and include:

1. Sense-making: the ability to comprehend and articulate the circumstances as a clear reference for effective decision-making.
2. Perspective-taking: the ability to see things from someone else's viewpoint, a critical element for social interaction and collaboration.
3. Issue-selling: the ability of directing attention to important issues.
4. Using creativity: the ability to generate out-of-the-ordinary and useful ideas, processes and procedures to achieve given objectives.
5. Fostering organizational agility: the ability to facilitate task completion thanks to a thorough understanding of business processes and units.
6. Communicating effectively: the ability to implement an effective communication strategy to keep stakeholders informed about the crisis status.
7. Decision-making: the ability to make quick and sound decisions while under pressure.
8. Risk-taking: the ability to take some level of risk while making decision under pressure.
9. Acting with integrity: the ability to engage in ethical decision making and behaviors.
10. Promoting resilience: the ability to restore the organization to its pre-crisis state and to help it be better off following the crisis than it was before.
11. Fostering learning orientation: the ability to put in place post-crisis learning and reflection activities.

2.3 Cyber crises and leadership competencies

As stated by Prevezianou (2021, p.55), cyber risks constitute "a new hotbed of potential crises". The increasing reliance on digital technologies is resulting in cyber risks having greater potential negative consequences on our society (Bonime-Blanc, 2021; Prevezianou, 2021). The rise of cyber crises has thus led to the creation of a new research stream in the crisis management literature.

Already twenty years ago, Boin (2004) framed cyberterrorism as one type of transboundary crises. According to Boin (2004), a transboundary crisis is a modern crisis that "thrives on fragmentation and variety. Its complexity defies governmental efforts to understand its causes, pathways, and potential remedies"; […] is not boxed in by set dates that mark a clear beginning and ending; it is an embedded vulnerability that emerges, fades, mutates, and strikes again". More recently, other works, such as those by Ansell et al. (2010) and Backman (2021) confirmed the nature of cyber crises as transboundary crises, characterized by rapidly escalating impacts that create spillover effects that cross multiple jurisdictions and borders, such as the physical/virtual one. Accordingly, Ansell et al. (2010) stated that to face cyber crises organizations need to be nimble and adaptive, robust and flexible, rapid in reacting and reorganizing their activities and courses of action; Backman (2021) further highlighted the need for technical expertise, creativity, pragmatic thinking and communication effectiveness to overcome this type of crises.

In this scenario, understanding exactly what leadership competencies an organization needs to structure and execute a cyber crisis management plan can be the differentiator between "cyberattack survival and extinction" (Golandsky, 2016). One of the first work in this field was that by Salviotti et al. (2023), that attempted to examine whether the leadership competencies identified in traditional crisis management literature are effective also in the context of cyber crises. The authors did so by applying the leadership competencies model developed by Wooten & James (2008) to the crisis that hit Norsk Hydro, a Norwegian company, in 2019.

While their results provide initial insights into understanding which are the relevant capabilities required to handle a cyber crisis, the same authors pointed out their limitations. Specifically, they highlighted how further research in this field could investigate other case studies that displayed other characteristics (different geography, response, etc.) to reveal additional or different leadership competencies. Thus, this paper aims to expand on the reference paper and advance knowledge in this critical field. By analyzing a new case study, different in terms of both sector and geography, this research aims to verify or challenge Salviotti et al.'s (2023) findings and potentially uncover previously unconsidered elements.

3. Methodology

In this section, we outline the methodology used for analyzing the case study, and the criteria for selection. In addition, we provide additional information about the selected case study.

3.1 Narrative inquiry approach

To achieve consistency with the results obtained by Salviotti et al. (2023), we opted for the same methodology used in their paper – Narrative Inquiry. Narrative Inquiry is an approach to research that seeks to understand and analyze the stories people tell about their experiences (Murray, 2009; Wells, 2011). One of its primary benefits is that it allows to capture the complexity and diversity of human experiences

(Murray, 2009; Wang & Geale, 2015). Furthermore, Narrative Inquiry 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; Savin-Baden & Niekerk, 2007). Leadership competencies can indeed be deeply understood through the stories and experiences of leaders (Flick, 2022; Gabriel, 2000). In this paper, Narrative Inquiry was used 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 them.

3.2 Case study selection

A crucial step in the research process was the selection of the case study that best fitted the research purpose. Multiple cases involving organizations victims of a cyber-attack were considered and compared according to the following criteria (Eisenhardt, 1989; Stake, 1995; Yin, 2018):

- Relevance: the case's ability to provide insight into the phenomenon.
- Information richness: the presence of detailed and comprehensive data about the phenomenon.
- Variability: the diversity in terms of context, settings, and stakeholders involved.
- Time frame: the case had to be prior to 2020, to allow the study of the post-crisis activities.
- Stakeholders involved: the case had to feature the active participation of leaders during the crisis.

Based on these criteria, the Maersk Global Supply Chain Meltdown case was selected. A.P. Moller-Maersk, commonly known as Maersk, is a global integrated logistics company that 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, where it started as a shipping company and expanded rapidly during the First World War. Over the years, Maersk diversified its operations, entering industries like oil and gas exploration. In 2016, the company underwent a strategic reorganization with a focus on becoming a specialized integrated transport and logistics company. By 2017, Maersk was a global leader in the industry, playing a major role in 343 ports around the world and managing about 18% of the world's container shipping.

In June 2017, the company was hit by the NotPetya cyber-attack. While the origins of the attack are still not entirely clear, NotPetya is widely believed to have been launched from Russia to sabotage Ukrainian infrastructures. In this context, the Maersk crisis can be seen as a side effect of a wider conflict, and as an example of how many cyber-attacks have unintended spillover effects on organizations.

The NotPetya attack on Maersk – also referred to as the Maersk Global Supply Chain Meltdown (Wesley et al., 2019) – forced the company to rebuild its entire IT infrastructure from scratch. Maersk needed approximately ten days to restore its essential business systems, and several weeks to fully recover.

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 actions helped to minimize the impact of the attack and restore operations as quickly as possible (Greenberg, 2017; Wesley et al., 2019). However, the incident was also an expensive wake-up call.

3.3 Data collection and analysis

To build the narrative and proceed with the analysis of the Maersk case study, multiple sources of data were used. It is important to emphasize that the narrative was not based on direct interviews, due to the impossibility of interviewing the company's personnel involved in the case. However, we believe that this did not limit the analysis excessively: the chosen case is characterized by a large amount of public information released by the top managers directly involved in all the activities conducted. These sources represent valuable data and were used as the main materials to build the narrative. They 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. Primary data include all the instances in which key employees of Maersk who played an active role during the NotPetya attack had the possibility to share their own perspective of what happened. Such employees are quoted during the analysis using their initials, and are Jim Hagemann Snabe, Maersk Chairman | {JHS}, Soren Skou, Maersk CEO | {SS}, Gavin Ashton, Maersk Identity & Access Management (IAM) service owner | {GA}, Bharat Halai, Maersk Head of IAM | {BH}, Adam Banks, Maersk CTO & CIO | {AB}, and Andy Powell, Maersk CISO | {AP}.

It is worth to emphasize that the all the key employees held 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 significant role in response to the crisis. Thus, their testimonies provide a 360-degree perspective of what happened, guaranteeing the validity and completeness of the narrative constructed.

To complete the narrative, several 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 analyzed to understand any changes in the company's strategic, organizational, and financial plan in response to the attack.

The construction of a narrative from collected data was the result of a progressive data analysis approach consisting of five stages: organizing and preparing the data, obtaining a general sense of the information, performing the coding process, categorizing into themes, and interpretating the data.

The initial stage of the analysis was organizing and preparing the data, and involved transcribing audio recordings of the podcasts, keynote speeches and panel discussions. In this phase, any non-narrative line and any contribution by other guests or speakers were excluded. The transcripts were then stored into a unique repository which was completed with additional quotes taken from selected secondary sources.

The second step was obtaining a general sense of the information. Passages and citations were organized and grouped according to the phase of the crisis to which they referred. This step also involved taking notes and making observations about the data, identifying recurring themes and patterns, and developing an initial coding scheme. This allowed to familiarize with the data and to start having a good understanding of the distinctive aspects of the case.

Subsequently, we proceeded to code, categorize, and interpret the data. In doing so, we followed the classical approach by Strauss & Corbin (1990), consisting in the three steps of open, axial, and selective coding. To follow these three steps, the transcripts were re-read to identify recurring words, ideas, or patterns. Prominent ideas and recurring words/messages were highlighted and corresponding first order concepts (FOCs) were developed. In total, 67 FOCs emerged. Axial coding was then performed, leading to the identification of 22 second order themes (SOTs). These themes were then grouped into 10 logical categories, the third order themes (TOTs) (see Table 3).

Table 3. Overview of 3rd-Order Themes (TOTs)

3rd-Order Themes (TOTs)
Technical ignorance
Organizational ignorance
Collaboration deficit
Network leverage
Organizational agility
Creativity
Effective decision-making under pressure
Open and ethical communication
Organizational learning
Organizational implementation

4. Findings

This section presents the data interpretation, which is the last step of the Narrative Inquiry approach described in the previous section. In this section, the TOTs are used as the starting point to analyze and interpret the Maersk case.

4.1 Overview of the attack

On June 27th, 2017, Maersk fell victim to the NotPetya cyber-attack. The malware infiltrated the company's system through the MeDoc software installed on a computer in Odessa, Ukraine. The attack forced the company to shut down its IT systems and disrupted business operations at many of its ports around the world. In response to the attack, Maersk's incident response team established an emergency recovery center in London. Hundreds of staff members worked tirelessly to rebuild the network, confiscating infected equipment and distributing new computers to the recovery personnel. However, they encountered a major setback when they realized that there was no clean backup of the company's domain controllers (a type of 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. 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 NotPetya. Eventually, the backup was hand-delivered to a Maersk employee in Nigeria, who then flew it back to London. During the recovery process, Maersk had to manage shipments manually, leading to a 20% decline in volume. However, the company's ships, largely disconnected from the network, continued their operations independently. As the network was restored, online ordering and tracking services were prioritized. It took about two weeks for port facilities to return to normal operations. The financial impact of the NotPetya attack on Maersk was significant, estimated between $250 million and $300 million. Additionally, locally stored information on infected PCs that hadn't been backed up prior to the attack was permanently lost.

4.2 Before the crisis

The Pre-crisis period covers all Maersk's activities starting from 2015 until the cyber-attack took place on June 27th, 2017. Three TOTs emerge from this stage of the crisis, namely Technical ignorance, Organizational ignorance and Collaboration deficit. All of them highlight the company unpreparedness both from the organizational perspective and the technical one.

In the years preceding the crisis, Maersk had started an intense digital transformation to redesign its processes and increase its competitiveness. However, a significant flaw in this digital strategy was the lack of awareness among managers regarding the risks associated with 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 needed to support the transformation. {GA} asserted 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 tools to support the digital strategy of the company sensibly contributed to increase its attack surface.

The technical ignorance was further amplified by the organizational one. Specifically, the top management lacked awareness about the importance of defining a solid cybersecurity strategy. This was evident from the words of {GA}, who said that "Shipping is a huge business but operates on relatively thin margins. IT had up until that point had been managed as a cost center to be minimized, rather than as a business enabler. In the race to the bottom, security controls had ultimately suffered and become a secondary concern to delivery". Security was not a relevant KPI for the organization, and all the activities related to securing Maersk's network were widely ignored. This type of ignorance had a domino effect on the entire company, generating a diffused lack of cyber awareness at all hierarchical levels. There were no pre-defined company-wide guidelines, policies or procedures 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 standardized and consistently applied privileged access controls made it trivial for notPetya to wipe Maersk out".

As for the collaboration deficit, a diffused lack of information sharing between top management and operative levels was indeed felt in all of Maersk's business units. This resulted into the IT staff experiencing strong difficulties in communicating about the relevance of vulnerabilities in the system. {GA} recounted that he spent two years "fruitlessly pushing for privileged access controls".

4.3 During the crisis

The proper crisis started on June 27th, 2017, when Maersk publicly declared on its official Twitter account that it was hit as part of a global cyber-attack named Petya. {JHS} said "I was woken up at 4 o'clock in the morning. A call came from the office that we had suffered a cyber-attack. 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 25th, 2017 Maersk published a global update on his website stating that the company was close to full recovery and that the majority of its global applications were back online and running (Wesley et al., 2019). Seven TOTs emerge from this stage of the crisis, namely Organizational ignorance, Collaboration deficit, Effective decision making under pressure, Network leverage, Open and ethical communication, Organizational agility and Creativity.

It is worth noting that the first two TOTs are the same described in the previous paragraph. 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 state of widespread confusion within all the business units around the world. The organizational leaders were unsure about which actions to implement in response 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". At first, it wasn't clear who was threatening the company, or what, or why. Chaos made impossible to get a realistic estimate of what was impacted and to which extent. This lack of visibility resulted into an initial collaboration deficit that caused employees to be left in the dark during the first days following the attack. However, even though at first they felt lost, Maersk's top managers rapidly took action to understand what was going on. One of the TOTs that emerges from this stage is indeed effective decision making under pressure. Top managers got involved in every crisis call to stay informed and make critical decisions. The presence and visibility of leaders made a big difference in responding to the attack. After the initial stalemate, decisions were taken in a very quick and efficient way, with the primary objective of achieving quick wins, even if that meant taking some risks without everything being flawlessly executed. Prioritization of business-critical processes was the key objective at this time.

Throughout the analysis, it also appears that open and ethical communication and network leverage were critical and interrelated factors in navigating the crisis. From the very beginning of the attack, Maersk adopted an open and transparent approach toward its clients, partners, and suppliers. That allowed the company to maintain a credible and consistent channel of communication and to avoid the risk of fake news. Being open and consistent in their external communications allowed Maersk to receive the help of its partners and customers, which were essential to

create a synergic network of shared skills and competences 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. […] Their first response was, how can we help?". Effective communication and network leverage played a big role in allowing Maersk to survive the attack: "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" {AB}. Eventually, its strong relationships allowed Maersk to also minimize the impacts on its 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".

The last two TOTs that emerge during this phase are organizational agility and creativity. The main factors behind the TOTs are human resilience and empowerment of people. 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. 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. 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, who did not have 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}. {GA} stressed that together with human resilience, a strong sense of collaboration and team-working allowed employees to effectively carry out their tasks despite the very severe conditions.

4.4 After the crisis

The Post-crisis stage starts about a month after the attack, when Maersk publicly declared it was going back to a normal situation. Three TOTs emerge from this stage of the crisis, namely Organizational learning, Organizational implementation and Network leverage. It's worth noting that the third TOT is the same described in the previous paragraph. However, in this stage it assumes a slightly different meaning.

The first TOT that emerges from the analysis is organizational learning. After the crisis, Maersk conducted an extensive analysis of their response to the attack, identifying lessons learned to enhance their practices and avoid similar mistakes in the future. The first major learning was the need to develop and nurture a new set of skills, tools and capabilities. As stated by {JHS} "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". Lessons learned from the cyberattack were also outlined by both {AP} and {AG}. In his speech on implementing the lesson learned from NotPetya attack, {AP} said that "it is a golden lesson in itself [learning] about how many of our third-party software suppliers represent quite a large risk to us". Other lessons learned concerned the importance of offline backups and the need to integrate cybersecurity into product development from day one. 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. […] [The second is] Everybody is responsible for security, okay? […] Third is trust. Build trust with your clients. […] Fourth is resilience. […] And finally, that security is a benefit, not a burden".

Alongside organizational learning, organizational implementation was the second TOT playing a key role after the crisis. Strategic investments were made to increase the cybersecurity posture of Maersk. A CISO – Andy Powell – was appointed, and he was assigned with the task of defining and implementing a cybersecurity strategy involving people, processes and technologies. Consequently, the required security tools and technologies were implemented, and company-wide cybersecurity frameworks and standards were defined. Acknowledging that an attack cannot be completely avoided resulted in the adoption of a proactive security approach. Citing {AP} words, "[…] We now have contingency plans at all our ports and terminals". In addition to that, {AP} also stressed the importance of adopting a risk-based approach to guide investments choices. As a result, Maersk's processes were redesigned according to the practices emerged during the attack. Furthermore, to respond to the need of new skills and competences, after the attack Maersk focused on hiring new talents.

The final TOT that emerges in this phase is network leverage. In fact, Maersk focused not only on implementing the lessons learned from the attack, but also on sharing them with all its external stakeholders. {AP} stated that "we have to share what we know about how these things work openly to stop them". After the crisis, Maersk leaders continued to participate to discussions and events to share their experience and

suggest best practices on how to approach cybersecurity. Their primary objective was to enhance awareness and ultimately establish a robust cybersecurity posture throughout the entire value chain.

5. Discussion

This section aims to link the TOTs that emerged from the analysis to the leadership competencies defined in the Wooten & James (2008) model. Each TOT is also showed in relation to the specific crisis stage(s) in which it emerged. The findings are summarized in Figure 1.

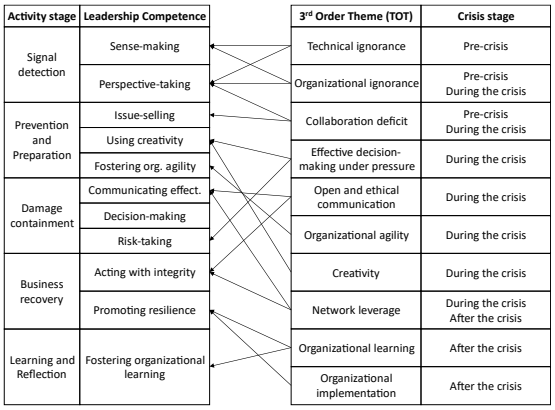

Figure 1. Application of the Wooten & James (2008) model to the Maersk case.

Figure 2 illustrates the relationship between the findings of the original model by Wooten & James (2008), the work by Salviotti et al. (2023) and those of the present study. Specifically, the figure provides detailed insight into whether the findings identified by Salviotti et al. (2023) are confirmed or not, as well as any additional findings that have emerged.

Leadership Competence	Contributions
Sense-making	• Confirmed Salviotti et al.'s (2023) assumption of relevance in the precrisis stage. • Furthermore, we pose that the two competencies are not only necessary before but also during the crisis.
Perspective-taking	
Issue-selling	• Confirmed Salviotti et al.'s (2023) assumption of relevance during all stages. • Furthermore, we pose that the three competencies are actually more useful during the crisis rather than before, as prescribed instead by Wooten & James' (2008) original model.
Using creativity	
Fostering org. agility	
Communicating effect.	• Confirmed Salviotti et al.'s (2023) assumption of relevance during all stages. • Furthermore, we highlight the role played by the external rather than only internal communication capabilities, referring to the capability of Maersk's leadership to leverage its network of customers, suppliers and partners.
Decision-making	• Confirmed Salviotti et al.'s (2023) assumption of relevance in the crisis stage.
Risk-taking	• Refuted Salviotti et al.'s (2023) assumption of doubtful relevance of the capability. • On the contrary, we pose that it resulted vital to avoid paralysis and respond to the attack.
Acting with integrity	• Confirmed Salviotti et al.'s (2023) assumption of relevance during all stages. • Furthermore, we highlight that acting with integrity can significantly contribute to increasing the company's leverage on its network of customers, suppliers and partners.
Promoting resilience	• Confirmed Salviotti et al.'s (2023) assumption of relevance in the crisis stage. • Furthermore, we pose that the competence is actually more useful after rather than during the crisis, as prescribed instead by Wooten & James' (2008) original model.
Fostering org. learning	• Confirmed Salviotti et al.'s (2023) assumption of relevance in the postcrisis stage.

Figure 2. Main contributions of the paper.

5.1 Signal detection

Three TOTs can be linked to this crisis phase. Technical ignorance and organizational ignorance are linked to both Sense-making and Perspective-taking; The third one, collaboration deficit, can only be linked 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 competencies, which could have allowed Maersk to anticipate the attack or take proactive steps to respond to it. It is worth noting that while in the original Wooten & James model (2008) the Sense-making and Perspective-taking competences relate only to the Pre-crisis phase, in Maersk case the ignorance and collaboration deficit TOTs emerge both before and during the crisis. This highlights that in cyber crises Sense-making and Perspective-taking competencies are necessary in both stages.

These results confirm and extend the reference paper findings. Managers who possess a heightened awareness of cyber risks are better equipped to fully comprehend the situation and make responsive and timely decisions.

5.2 Prevention and preparation

Regarding this phase, what emerged is how the Issue-selling competence is linked to the collaboration deficit TOT. Before the attack, Maersk middle managers and IT staff were experiencing great difficulties in communicating to top managers about the alarming cyber risk exposure of the company. 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 competences emerge as directly linked to the homonymous TOTs. However, in the Maersk case both played a fundamental role during the crisis, rather than before as described in James & Wooten (2008) model. This is also in line with Salviotti et al. (2023). The same applies to Using creativity. In the case, the ability to use out-of-the-ordinary solutions was essential to ensure business continuity when the traditional methods were completely disrupted. Thus, the Maersk case supports the original authors finding that organizational agility and creativity "are found to be useful also and above all during the crisis".

5.3 Damage containment

In Maersk case, the first and the third competencies highlighted in the Wooten & James (2008) model are strictly related to the effective decision-making under risk and pressure TOT. The company response to the crisis highlights that the ability to make decisions under pressure, and to take risks to prioritize activities, allowed leaders to achieve quick wins and contain the impact of the attack. This finding not only supports the reference paper results, but also extends them. While in

Salviotti et al. (2023) "it was not possible to trace a precise connection between 3rd-order theme and the risk-taking capability", in Maersk case the leaders' ability of making decisions under uncertainty resulted vital to avoid paralysis and respond to the attack.

As for Communicating effectively, this can be linked to the TOT of open and effective communication. 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 helped Maersk to minimize the potential losses from the attack.

The network leverage TOT is also related to the same competence. While in the reference paper this specific aspect is not discussed, in Maersk case effective communication helped the company to leverage its rich network of customers, suppliers and partners. This network turned out to be essential during the crisis as it allowed to share skills, competences, and technologies that Maersk was lacking, and that were fundamental to respond to the attack.

5.4 Business recovery

The promoting resilience competence can be linked to both TOTs of organizational learning and organizational implementation. Maersk's leaders approached the crisis as a catalyst to think differently about the organization, with the goal of making it better off than as it was before and keeping it ready to face future adversities. This confirms the findings of the reference paper. As for Acting with integrity, this competence is linked with the open and ethical communication TOT and to the network leverage one. While Salviotti et al. (2023) found this competence to be among the most relevant after the crisis, from our analysis it emerges that it was fundamental since its beginning. In the Maersk case, the leaders' ability to engage in ethical and consistent communication was crucial both during the crisis to keep the trust of the stakeholders involved, and after the crisis to keep them involved in the learning activities.

5.5 Learning and reflection

The competence of Fostering organizational learning aligns perfectly with the organizational learning TOT, supporting the findings of the reference paper. In the Maersk case, the main lessons to be learned were the need to recognize cybersecurity as a source of future competitive advantage, and the need to develop new skills, tools and capacities to enhance the cybersecurity posture of the company. These learnings influenced all the activities performed after the crisis.

As for the TOT of organizational implementation, differently from the reference paper we argue that this should be linked to the Promoting resilience competence – which, however, should be present both during the crisis and after, contrarily to what prescribed by Wooten & James (2008) that only reference it in the crisis stage.

6. Conclusions

The proliferation of digital technologies in recent years led to an increase in cyber crises. Despite the relevance of the topic, literature in the field of crisis management is still deficient when it comes to providing a solid understanding of how to effectively handle a cyber crisis. Based on a model developed by Wooten & James (2008) on crisis management leadership competencies, Salviotti et al. (2023) started filling this gap by evaluating the role of such competencies in the context of cyber crises. Building upon their research, this paper extends the analysis to the Maersk case and confirms most of the findings of the reference paper, while additionally uncovering new elements.

One major insight that emerges is the need for Sense-Making and Perspective-taking competencies not only before the crisis, but also during it. In fact, poor managerial ability to foresee the implications of cyber risks may not only hinder prevention and preparation actions, but also paralyze the organization in the immediate aftermath of an attack. Additionally, the analysis highlighted the importance of Risk-taking to make timely decisions during the crisis, and revealed a further competence, that of leveraging a strong network of external stakeholders. While some competences mentioned in the original Wooten & James (2008) model – such as Communicating effectively and Acting with integrity – already took into consideration network effects, the Maersk case highlighted the important role played by its customers, suppliers, and partners in actively solving the crisis. Finally, we argue that the Promoting resilience competence should be present both during and after the crisis.

By validating the findings by Salviotti et al. (2023) and extending them, this paper contributes to advancing knowledge in the field of cyber crisis management and supports organizations in their efforts to understand this phenomenon.

6.1 Limitations and further research

The main limitation of this paper arises from the reliance on secondary qualitative data for data collection. Although we believe that the abundance of available data partially mitigated this limitation, there is potential for future research involving directly key stakeholders to further enhance the understanding of the

Maersk case study. Furthermore, it is important to note that cyber crisis management remains a research area insufficiently explored. Future research streams should aim to build upon and consolidate the existing knowledge by conducting additional studies in different organizational settings and industries.

7. References

Backman, S. (2021). Conceptualizing cyber crises. *Journal of Contingencies and Crisis Management*, *29*(4), 429–438.

Bibeault, D. B. (1998). *Corporate Turnaround: How Managers Turn Losers Into Winners!* (pp. 17–18). Beard Books.

Boin, A. (2004). Lessons from crisis research. *International studies review*, 6(1), 165-194.

Boin, A., Kuipers, S., & Overdijk, W. (2013). Leadership in Times of Crisis: A Framework for Assessment. *International Review of Public Administration*, *18*(1), 79–91.

Bonime-Blanc, A. (2021). Cyber organizational resilience is a business imperative: The essential eight steps to get there. *Actuarios*, *48*.

Bundy, J., Pfarrer, M. D., Short, C. E., & Coombs, W. T. (2017). Crises and Crisis Management: Integration, Interpretation, and Research Development. *Journal of Management*, *43*(6), 1661–1692.

Butina, M. (2015). A Narrative Approach to Qualitative Inquiry. *American Society for Clinical Laboratory Science*, *28*(3), 190–196.

Coombs, Timothy, & Holladay, S. (2001). An Extended Examination of the Crisis Situations: A Fusion of the Relational Management and Symbolic Approaches. *Journal of Public Relations Research*, *13*(4), 321–340.

Coombs, W. T. (2023). *Ongoing Crisis Communication*. SAGE Publications.

Duchek, S. (2020). Organizational resilience: a capability-based conceptualization. Business research, 13(1), 215-246.

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. *The Academy of Management Review*, *14*(4), 532–550.

Fink, S. (1986). *Crisis Management: Planning for the Inevitable*. American Management Association.

Flick, U. (2022). *An Introduction to Qualitative Research*. SAGE.

Gabriel, Y. (2000). *Storytelling in Organizations: Facts, Fictions, and Fantasies.* Oxford University Press.

Golandsky, Y. (2016). Cyber crisis management, survival or extinction? *2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*, 1–4.

Greenberg, A. (2017, August). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*, *22*.

James, E. H., Wooten, L. P., & Dushek, K. (2011). Crisis Management: Informing a New Leadership Research Agenda. *The Academy of Management Annals*, *5*(1), 455–493.

Liu, Y., Shankar, V., & Yun, W. (2017). Crisis Management Strategies and the Long-Term Effects of Product Recalls on Firm Value. *Journal of Marketing*, *81*(5), 30–48.

Mitroff, I. (1994). Crisis Management and Environmentalism: A Natural Fit. *California Management Review*, *36*(2), 101–113.

Murray, G. (2009). Narrative Inquiry. In J. Heigham & R. A. Croker (Eds.), *Qualitative Research in Applied Linguistics: A Practical Introduction* (pp. 45–65). Palgrave Macmillan UK.

Pearson, C. M., & Clair, J. A. (1998). Reframing Crisis Management. *Academy of Management Review*, *23*(1), 59–76.

Prevezianou, M. F. (2021). Beyond Ones and Zeros: Conceptualizing Cyber Crises. *Risk, Hazards & Crisis in Public Policy*, *12*(1), 51–72.

Robert, B., & Lajtha, C. (2002). A New Approach to Crisis Management. *Journal of Contingencies and Crisis Management*, *10*(4), 181–191.

Salviotti, G., Abbatemarco, N., De Rossi, L. M., & Bjoernland, K. (2023). Understanding the Role of Leadership Competencies in Cyber Crisis Management: A Case Study. *Proceedings of the 56th Hawaii International Conference on System Sciences*, 6068–6078.

Savin-Baden, M., & Niekerk, L. V. (2007). Narrative Inquiry: Theory and Practice. *Journal of Geography in Higher Education*, *31*(3), 459–472.

Stake, R. E. (1995). *The Art of Case Study Research* (pp. 49–71). SAGE.

Strauss, A., & Corbin, J. M. (1990). *Basics of qualitative research: Grounded theory procedures and techniques.* SAGE.

Van Der Vegt, G. S., Essens, P., Wahlström, M., & George, G. (2015). Managing Risk and Resilience. *Academy of Management Journal*, *58*(4), 971–980.

Van Wart, M., & Kapucu, N. (2011). Crisis Management Competencies. *Public Management Review*, *13*(4), 489–511.

Wang, C. C., & Geale, S. K. (2015). The power of story: Narrative inquiry as a methodology in nursing research. *International Journal of Nursing Sciences*, *2*(2), 195–198.

Wells, K. (2011). *Narrative Inquiry*. Oxford University Press.

Wesley, D. T. A., Dau, L. A., & Roth, A. (2019). *Cyberattack: The Maersk Global Supply-Chain Meltdown*. Harvard Business Review Case Studies.

Williams, T. A., Gruber, D. A., Sutcliffe, K. M., Shepherd, D. A., & Zhao, E. Y. (2017). Organizational response to adversity: Fusing crisis management and resilience research streams. *Academy of management annals*, 11(2), 733-769.

Wooten, L. P., & James, E. H. (2008). Linking Crisis Management and Leadership Competencies: The Role of Human Resource Development. *Advances in Developing Human Resources*, *10*(3), 352–379.

World Economic Forum. (2023). *Global Risks Report 2023*. https://www.weforum.org/reports/global-risks-report-2023/

Yin, R. K. (2018). *Case study research and applications: Design and methods (6th ed.)*. SAGE.