Understanding the Role of Leadership Competencies in Cyber Crisis Management: A Case Study

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

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

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

Kaia Bjoernland
Università Bocconi
kaia.bjoernland@studbocconi.it

Abstract

The amount and severity of cyber-attacks has been constantly increasing in recent years, and the number of cyber-related organizational crises grew accordingly. Despite the relevance of the topic, the literature on the subject is still limited, especially from a non-technical point of view. In the context of leadership, traditional crisis management literature identified specific competencies that organizations can leverage to mitigate the effects of a crisis, but there is a research gap as to whether or not these capabilities make sense in a cyber crisis context. This study aims to bridge this gap by analyzing the case of Norsk Hydro – a Norwegian company that in 2019 fell victim of a disruptive ransomware attack – through the lenses of a traditional crisis leadership model.

Keywords: Cybersecurity, Cyber Risk, Organizational Crisis, Crisis Management, Crisis Leadership

1. Introduction

The emergence of the World Wide Web transformed the world, arguably for the better and the worse. In a relatively short period of time, our relationship with information technology has progressed from being sporadic to an omnipresent necessity in virtually all our lives (Holt & Bossler, 2015; Iansiti & Lakhani, 2014). The increasing dependency on technology has simultaneously given rise to opportunities for malicious users of the internet. Resultingly, cyber-crime is quickly becoming one of the fastest-rising forms of modern crime (Wall, 2013).

One of the most pressing concerns within cybercrime is the rapid evolution of ransomware. Ransomware is a particular type of malicious software designed to block access to a computer system until a sum of money is paid (Connolly & Wall, 2019). Ransomware evolved from being a niche cybercrime to one of the greatest threats for both governments and corporations (Ryan, 2021). From the first observed major attack in 2013, ransomware had by 2016 become a global epidemic for these targets. Indeed, the world saw a 105% increase in ransomware attacks in 2021, and the average cost for remediation more than doubled between 2019 and 2020 – from around $750k to $1.85 million (Sonicwall, 2022; Sophos, 2021). The foregoing statistics shed light on another alarming concern, namely organizational insufficiency of understanding and protecting themselves against ransomware attacks. What many refer to as a race between cybercriminals and organizations might currently be led by criminals. As a result, more and more organizations in the coming years will have to face a crisis triggered by a cybercrime (Goutam, 2015; Ponemon Institute, 2021).

The existing literature on crisis management describes the factors behind an organizational crisis as "characterized by surprise" and implies that they can "hold value for the organization, both in a positive and a negative sense" (Bechler, 1995). Several authors have tried to categorize these factors to help the organization "minimize the negative impacts of crisis or by leveraging the crisis situation to its advantage" (Bhaduri, 2019). Organizational culture and human factors are often considered as among the most influential ones, and the literature claims that effective leadership, coordinated teams and motivated employees can have a great effect on averting and controlling crisis (Bhaduri, 2019; Denis et al., 2001; Sun, 2008; Wang & Belardo, 2005).

Considering the increase in the spread and severity of cybercrimes globally, it is reasonable to assume that understanding what leadership competencies prove to be more effective in cyber-

URI: https://hdl.handle.net/10125/103370
978-0-9981331-6-4

related crises can provide valuable insights to both scholars and practitioners. However, given the relatively recent nature of the topic, there is currently a wide research gap in this area.

The following study aims to contribute to fill this gap by applying the lens of crisis management to a case study that become quite famous in recent years: that of Norsk Hydro, a Norwegian company hit by a ransomware attack in March 2019.

In view of the foregoing, the main question guiding this research is:

RQ: How do leadership competencies contribute to mitigate the negative impacts of a cybersecurity crisis?

The study aims to answer this question by applying the crisis management leadership competencies model developed by Wooten & James (2008) to the analysis of the Norsk Hydro case, which was analyzed for the purposes of this study through a narrative inquiry.

The structure of this work is as follows. First, in section 2 we provide a concise literature review on the current cybercrime and ransomware scenario, on crisis management and on the leadership competencies needed to manage crisis. In section 3, we describe the methodology used in the study, as well as the data collection details. In section 4, we analyze the Norsk Hydro case, whose findings are then presented in section 5. Finally, in section 6 we present our concluding remarks and the limitations of the research.

2. Literature review

2.1. Cybercrime and ransomware

Cybercrime is quickly becoming one of the fastest-rising forms of modern crime, and a growing phenomenon within the literature (Batra & Gupta, 2020). Belonging to the category of cybercrimes, ransomware is currently one of the most pressing concerns in the realm of cyberthreats (Couburn et al., 2018). This is because ransomware poses a greater existential threat to corporations than other forms of cyberattacks (Ryan, 2021). The term ransomware is derived from two words – ransom and malware (Mohammad, 2020): this is because a ransomware can be considered as a particular type of malware whose primary aim is to extort ransom payments from users (McIntosh et al., 2022). Malware, in turn, is an abbreviated term for Malicious Software, specifically designed to gain access to or damage victims' machines (Mohammad, 2020).

Thus far, scholars and IT professionals have been unable to derive a practical and cost-effective method to prevent successful ransomware attacks (Ryan, 2021). This is becoming more and more critical with cyberattacks growing in frequency, scope, and ambition (Couburn et al., 2018). The insufficient knowledge regarding ransomware, both from a conceptual and practical perspective, highlights the necessity of a further examination of this phenomenon (Backman, 2021).

2.2. Crisis management

Defining "crisis" is challenging, due to its inherently interdisciplinary nature. Consequently, the term carries many meanings and there are discrepancies regarding its constitutional elements. One of the most widespread interpretations is that by Pearson & Clair (1998), which define organizational crises as "*low-probability and high-consequence events*" and as "*generally characterized by ambiguity*". Accordingly, a crisis involves a period of discontinuity, wherein the core values of the organization are under threat, and critical decisions need to be taken (Holla et al., 2018). However, crisis management researchers are not focused only on the post-crisis period. Most researchers divide a typical business crisis into three or five phases. For example, Roux-Dufort (2007), argue that crisis management is a proactive process involving three stages: before the event triggering the crisis, throughout its course, and in its aftermath. Mitroff & Pearson (1993) provide five phases: signal detection, preparation and prevention, damage containment, recovery, and learning (Coombs, 1999; Pheng & Ann, 1999), according to the activities planned for each stage. Other scholars, such as Bhaduri (2019), consider both perspectives.

Like general crisis management, also cyber crisis management is characterized by a non-standardized terminology. Resultantly, there is no public agreement on the term, which indicates that there is a need for further investigation (ENISA, 2014; Prevezianou, 2020; Backman, 2021). The European Union Agency for Cybersecurity (ENISA) proposed the following definition for a cyber crisis event: "*A serious threat to basic structures or the fundamental values and norms of a system (in cyberspace), which under time pressure and highly uncertain circumstances necessitates making vital decisions*" (ENISA, 2014). The organization further stated that "*the crisis itself is not a threat but rather the result of a threat to any number of critical values*". These values go beyond the technical operation of various IT systems, as they may also include, for example, public faith in system

reliability, which remains compromised after the technical restoration.

2.3. The role of leadership competencies for crisis management

The relevance of leadership competencies during a crisis has been highlighted by several authors (Bhaduri, 2019; Denis et al., 2001; Sun, 2008; Wang & Belardo, 2005). Both Dutton & Jackson (1987) and Wooten & James (2004) argued that "*the effective management of an organizational crisis is dependent on leadership behaviour that encourages members to actively engage in knowledge acquisition and the formulation of strategies to resolve the crisis*" and that "*when these competencies are enacted, the likelihood that the firm will be resilient following the crisis is greatly enhanced*". Despite the importance of leadership competencies in a crisis management context, several studies have confirmed the lack of appropriate learning and training tools, which as a result leaves leaders unprepared. In particular, studies on the subject underline how processes such as sense-making, decision-making, and risk-taking are systematically underestimated (James & Wooten, 2005; Shaw & Harrald, 2004). Wooten & James (2008) argue that, although communication skills are fundamental, crisis management requires a broader skillset to overcome the various phases of the crisis and bring the organization to a successful recovery (Bolman & Deal, 1997; Burnett, 2002; Wooten & James, 2004), and that "*in its most ambitious form, crisis leadership is also about handling a crisis in such a way that the firm is better off after a crisis than it was before*" (Brockner & James, 2008; Wooten & James, 2004). Referring to the phases of crisis management provided by Mitroff & Pearson (1993), Wooten & James (2008) also tried to identify exactly what leadership competencies are required to face the critical tasks and activities typical of a crisis situation. These are briefly summarized in Table 1 below.

Table 1. Leadership competencies in crisis management according to 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
	Making decisions
	Taking risks
Business recovery	Acting with integrity
	Promoting resilience
Learning and reflection	Fostering org. learning

Since the topic of cyber crisis management is still relatively young and unexplored (Prevezianou, 2020; Backman, 2021), there is very little literature on what leadership competencies are needed during a cyber crisis event. For instance, it is not clear whether a cyber crisis requires the same leadership competencies needed in a generic crisis, given the peculiar characteristics of the former. Prevezianou (2020) assumes that elements such as the absence of clear boundaries, the alteration of the traditional crisis' time sequence, the presence of legitimacy and authority vacuums, and the greater escalatory and damage potential due to its complexity make a cyber crisis a transboundary crisis. As such, a cyber crisis may require additional leadership competencies and a different timing compared to a "traditional" one.

Our work aims to bridge this gap by assessing the consistency of the leadership competencies identified by the existing literature with respect to the specific cyber crisis context. In particular, we do so by applying the leadership competencies model developed by Wooten & James (2008) to a real-life cyber crisis scenario.

3. Methodology

3.1. Narrative Inquiry

To best answer the research question, the authors believed it was essential to capture the relevant actors' experiences with a cyber-related crisis. Consequently, the narrative inquiry was considered as a suitable methodology. Narrative inquiry is a form of qualitative research in which stories themselves become raw data. Therefore, the collection of narratives from individuals or groups is central to the respective research approach (Butina, 2015; Webster & Mertova, 2007). These narratives can be collected through various means including interviews, documents, and observations (Butina, 2015; Webster & Mertova, 2007). This study used the former two and excluded the latter due to the lack of direct access to the examined organization.

A crucial step in the research process was to select the appropriate case to contribute an increased understanding of leadership competencies in cyber crisis management. The initial research revealed a huge assortment of cases – that is, organizations being attacked by ransomware. However, there appeared to be a lack of cases that displayed both honesty and transparency about the attack, the crisis, and the approach to recovery. A case study which displays both honesty and transparency is not solely interesting from a research perspective, it also offers convenience in terms of an enlarged base of available information.

The latter represents one of the pre-determined case-selection criteria, namely access (Hay, 2016). Another criterion was to select an organization that was attacked by ransomware prior to 2020, as this would allow for the study of the post-crisis timeframe as well. Lastly, the authors wanted to select a crisis event in whose resolution the management played an active role, in order to obtain valuable insights on the role of leadership competencies in such scenario. Based on these criteria Norsk Hydro, was identified as the most suitable case.

3.2. Norsk Hydro

Norsk Hydro (or simply Hydro) was founded in 1905 by Norwegian entrepreneurs Sam Eyde and Kristian Birkeland. In the first years of its life, the company produced artificial fertilizers by utilizing hydropower to capture nitrogen from the atmosphere. When this process became obsolete, the company moved into new markets: in 1934, it created the first commercial plant for heavy water (a form of water that contains only deuterium rather than the common hydrogen-1 isotope), and in 1940 it entered the metal production sector. In 1965, the company also expanded into Oil & Gas, but this business was later spun off from the company and merged with Norwegian company Statoil in 2007. Three years earlier, Hydro had also spun off its fertilizer business as a separately stock-listed company under the name of Yara International. Today, Hydro is a global supplier of aluminium which employs approximately 31,000 employees in 40 countries and produced in 2021 a revenue of NOK 28 billion.

On March 19th, 2019, Hydro faced an extensive ransomware attack (Leppanen et al., 2019). When the ransomware attack was launched it compromised 22,000 computers across 170 different sites and 40 countries. Resultantly, employees at Hydro (35,000 at the time) restored all systems to manual production and in many cases production lines had to stop (Tidy, 2019). Overall, the cost of the attack was estimated to be between NOK 400-450 million due to loss of production and associated costs.

Hydro's response to the crisis became famous in the cybersecurity industry for its success and in the following years it became a sort of "the gold standard" for the sector. Norks Hydro refused to pay the requested ransom, while also handling the situation honestly and transparently. The company's stock price increased in the aftermath of the event, indicating that also investors appreciated the way Hydro handled the situation (Loeb, 2019).

3.3. Data collection

In order to proceed with the narrative construction, this study collected data through interviews and documents. It is important to highlight that the authors were unable to interview any of the members of Norsk Hydro top management directly. However, three of them, namely Inger Sethov (Head of Communication), Torstein Are (Chief Information Security Officer), and Halvor Molland (Information Director) had each participated in a webinar and two separate podcasts about the cyber-attack on Hydro. Both the webinar and the podcasts provided suitable narratives for the phenomenon under study. These three secondary interviews represent this study's main data. In the following sections, quotes or references ascribed to each of the three will be referred to with their respective initials {IS}, {TA}, {HM}. Additional secondary data sources such as official web pages, online news, and public documents have been used to detail the case and the relevant context. Hydro's annual reports from 2017 to 2021 were used to provide an understanding of how the company has evolved starting from one year prior to the attack, to three years later.

3.4. Data analysis

Narrative researchers usually assume the story to be the fundamental unit accounting for human experience. However, the kind of narrative, the methods used for narrative analysis, and the way the narrative is represented tend to vary (Moen, 2006; Webster & Mertova, 2007). This study uses a narrative inquiry to examine the Norsk Hydro case, in which content within the text is the primary focus (Butina, 2015; Webster & Mertova, 2007). In particular, the narrative thematic analysis used in this study is one suggested by Butina (2015), which consists of the following five stages: (I) organizing and preparing the data, (II) obtaining a general sense of information, (III) executing the coding process, (IV) categorizing into themes, (V) interpreting the data.

The organization and preparation of data began with transcribing the interviews. The interviews with Torstein Are and Halvor Molland were originally conducted in Norwegian and Swedish respectively and were therefore carefully translated to English. Thereafter, non-narrative lines were deleted, that is, casual conversations and contributions from the podcast hosts and the co-guest. In doing so, the resulting data was solely a contribution from Hydro's emergency team. The next step was then to transfer the transcripts into a common repository, where the transcripts were divided based on rudimentary

patterns. In the repository, additional quotes from external articles and videos from Hydro's CyberHeroes campaign were included as supporting data elements for the three main interviews. Following the first two steps, the authors proceeded with the coding process. The coding was performed in three main steps:

1. Open coding: detailed reading of the raw data and attachment of suitable codes, primarily based on the various phenomenon mentioned (First-Order Concepts). In the analysis, 63 first-order themes were identified.
2. Axial coding: clustering of the codes identified during the first step under higher-order sub-themes (Second-order themes). These are broader categories which are closer to the constructs of interest. 24 second-order themes were identified.
3. Selective coding: identification of the core elements around which second-order themes can be grouped. Ten third-order themes were identified.

Table 2. Overview of 3rd-Order Themes

3rd-Order Themes
Technical ignorance
Organizational ignorance
Collaboration deficit
Organizational alignment
Creativity
Decision-making under pressure
Effective communication
Openness and ethical behavior
Organizational learning
Organizational implementation

4. Analysis

This section analyses the response to the ransomware attack on Norsk Hydro from 2017 to 2021. The section first illustrates an overview of the event and then distinguished between three crisis management phases: before, during, and after the attack.

4.1. Overview of the attack

The ransomware that infected Norsk Hydro is called LockerGoga, which became known in 2019 when it infected Altran Technologies in France. After gaining access, LockerGoga denies users access, while also encrypting stored files. Thereafter the respective ransomware finishes its mission by disabling network access, before leaving a README_LOCKED.txt file on the desktop with a ransom note. As a result, Hydro needed to rebuild its entire IT infrastructure, in which they had invested 20-30 years of development, in a manner of months (Tidy, 2019).

However, as several Hydro employees have mentioned *"This was not an IT crisis, this was a company crisis"*. This is reflected in the disconnection of all the company's plants and operations, and its shift to manual operations. Out of Hydro's five largest departments, Extruded Solutions were hit the hardest followed by Rolled Products. Despite the setback, the former operated nearly at 100%, and the latter at about 50% of normal capacity two days after the attack. Hydro is accrediting this to its workforce's morale and spirit. This is illustrated in employees' willingness to spend extra hours and take on unconventional roles and responsibilities to help the company towards recovery (Tidy, 2019).

Hydro's initial emergency response is outlined as follows by {IS}. The attack was discovered in the US just after midnight before it travelled to Hungary in Europe where the IT infrastructure center of Hydro is located. {IS} stated that around 3 am the company's head of infrastructure made an independent and crucial decision to shut down 23,000 PCs and 3,000 servers. At 7 am, the communication principles "proactive, transparent and frequent" were decided upon. The top management then provided a stock exchange release prior to 9 am. By 3 pm the same day, Hydro held its first external webcast. This timeline illustrates that major decisions needed to be taken in a very time-pressured environment characterized by major uncertainties.

4.2. Before the crisis

This first period goes from 2017 to March 19th, 2019. In the present case study, all 3rd-order themes related to this phase revealed a diffused unpreparedness. This "ignorance" was evident at both the technical and organizational levels. At the technical level, the main factors included the lack of IT systems security measures, weaknesses in end-point security and monitoring, suboptimal architecture, and insufficient data backups. At the organizational level, "ignorance" was displayed through an acknowledged weakness in the company cybersecurity strategy, directly related to its lack of cyber awareness amongst employees. It is reasonable to argue that, prior to 2019, Hydro's top management neglected cybersecurity, resulting in an insufficient strategy and overall awareness. The analysis also identified a collaboration deficit, which is explained through a lack of information sharing between different stakeholders in the organization. Referring to the annual report analysis, it is evident that Hydro's cybersecurity focus was limited to Ordinary Defense

Capabilities (ODC), defined by Ferdinand (2015) as *"the front line of cyber defense, and the most basic level required to build cyber resilience"*. These basic capabilities translated into optional and limited training exercises and the acknowledgment of a risk exposure without a concrete strategy to mitigate it.

4.3. During the crisis

The proper crisis phase starts from the date of the attack and lasted for the following three months, when on July 19th, 2019, the IT department declared a transition from crisis mode to normal mode {TA}.

One of the first element to emerge in this phase is organizational alignment, resulting from a high degree of organizational agility and culture; both helped Hydro navigate the triggering event. *"Our culture, in which every single employee was prepared for and willing to work the extra mile, (...) helped us a lot."* {HM}. {IS} also stated how *"if you are open and transparent about what you do, but also about what you don't know, that is extremely good for morale and makes people help you solve the problem rather than working against you".*

Throughout the analysis, it also appears that "creativity" was a crucial factor in navigating the crisis. {HM} declared that *"creativity is a big and crucial component in these kinds of situations"*, followed by {IS} stating that *"it is interesting how you become creative when nothing works"*. Indeed, as Hydro did not have access to any of their normal means of communication, they resorted to other solutions such as WhatsApp and handwritten posters for internal communication, and Facebook and Twitter for external communication. Creativity was also used to generate motivation and engagement amongst employees. This is evident in Hydro's CyberHeroes campaign, which involved former employees brought back to aid with the creation of manual operations, or employees like Jan: *"Jan, a technology pessimist, always hated computers, hated IT. What he did was to print out all orders and all specifications throughout all the years he had been in Hydro. From being the technology pessimist, he became a hero because he had it all lined up. We lifted him up and talked about him internally to inspire other people"* {IS}.

What also emerged in this phase was the ability of Hydro management to act under pressure while still following transparent and ethical guidelines. Decision-making during the crisis was based on displaying trust and clearly delegating roles and responsibilities to produce outcomes immediately: *"I am part of the corporate emergency team in Hydro that is very well functioning, and we have been through many crises together and we have very clear roles and responsibilities in that team. In a crisis the only thing you don't have is time. You don't have time to question each other's roles and question each other's capabilities and mandates. You have to do your job and trust each other. And that trust is built over time, but it is also built by having clear roles and responsibilities within that team"* {IS}.

Following is the theme of effective communications. The criticality of communications is evident in the following statement by {IS}: *"I think that one of the success factors was that we decided to have daily internal updates. So, every morning we started with an internal update at nine o'clock even if we didn't have anything new to say. Here people could ask questions. Then we recorded it and then we put it out on the news app so that people who woke up in different time zones of the world could see the most recent update from Hydro"*. Additionally, this illustrates Hydro's emphasis on two-way communication, emphasizing the importance of erasing barriers to ask questions and raise concerns. {IS} goes on to talk about two crucial factors facilitating the success of their internal communication effort, namely "plain language" (*"The head of IT speaks in a way that we all understand, and this kept us more calm and happy during the crisis"*) and "humour" ("*So, we put down a lot of work to get people on board and make them understand and just create some laughter really helped the mood and the spirit and made sure that we kept on moving."*).

Having a pre-established communication plan guiding the company's internal and external communication was also essential to Hydro's response. *"Communication is part of our crisis team. In a crisis, it is key to establish a communication strategy and stick with this during the crisis. This is something we were prepared for and had trained on. So also in this crisis, which was a cyber crisis, we established a communication strategy. So being open, transparent, and providing timely information internally and externally was important from the very beginning"* {TA}. Communication efforts were especially effective with the company's customers: *"We have 30,000 customers around the world, and they were all concerned that they would not get their deliveries. So, what we decided very early on was to be frequent, direct, and open with our customers and give them updates on what was happening. What we saw was that customers were pleased that we were open from the start and that we were always available for questions. By being transparent we gained trust from our customers and therefore lost very few"* {IS}. Evidently, the overarching theme of openness and transparency was also reflected in the communication efforts with customers.

4.4. After the crisis

This period goes from July 2019 to the end of 2021. To improve their cybersecurity posture, it was imperative for Hydro to analyze data from the 2019 cyberattack to identify key points of error and improvements. Hydro's key learnings can be summarized in a need for increased cyber awareness and for a coherent organizational cybersecurity and cyber resilience strategy.

The key learnings are evident in the following statement by {HM}:*"(...) Our IT department regularly sends out test emails and there is always one or more that opens such emails. You cannot be safe 100%, you need a combination of awareness at the employee level and that the organization does its homework on how a cyber-attack can be avoided and what we will do if we are attacked. […] The most important learning is to be prepared and have thought through the problem in advance. When you are experiencing it, it is too late. And also make sure that you have good backup routines, so you have the possibility to go on with operations. In the best case, try to avoid it. And here cyber awareness amongst employees is key."*

Throughout the case study, some specific learning points on how to deal with future crises also appear. The following statement by {TA} indicate a general need to prepare for crisis management in more detail: *"People become very engaged in these kinds of situations – both our employees and our partners. They come to work and go the extra mile. This works for a week or two. But after that, people start to collapse. So it is crucial to get structures in place for shift work, make sure people get to rest and make sure that food and drinks are available. In general, make everything else convenient for the employees. This is something we will improve next time – have more of these things planned for in advance. […] We are confident that the top management crisis team works well but within IT and security we can plan for better systems and crisis management processes."*

Organizational implementation refers instead to the concrete measures Hydro took to embed the key learnings into the organization. A crucial element for analyzing organizational implementation were the annual reports from 2019 to 2021. As previously mentioned, in 2019 Hydro's cybersecurity strategy was limited to ODCs, indicating a low degree of cyber resilience maturity. In 2020, it becomes apparent that Hydro started to emphasize crisis management through the creation of ExtraOrdinary Capabilities (EOC) (Ferdinand, 2015), not related to day-to-day activities but rather to more extreme situations such as crises. EOC-building involves the creation of an emergency plan, and the identification of people to mitigate the crisis while raising staff level awareness and knowledge. In 2020 the development of ODCs and EOCs is evident through *"crisis management workshops"*, *"end-user awareness through e-learning"* and *"mandatory training for 11,000 employees"*. Hydro also emphasized that cybersecurity was on the board's agenda. The 2021 report reveals that Hydro further increased its focus on crisis management and EOCs development through the following additional measures: *"crisis anticipation and preparation"*, *"emergency preparedness plans"*, *"creation of a cyber crisis team"*, and *"crisis management training and capability building"*.

5. Findings

The present section seeks to answer to the study research question by associating the 3rd-order themes emerged during the narrative analysis and discussed in the previous session to the leadership capabilities in crisis management prescribed by the Wooten & James (2008) model. The table below summarized the results which are presented in the following paragraphs.

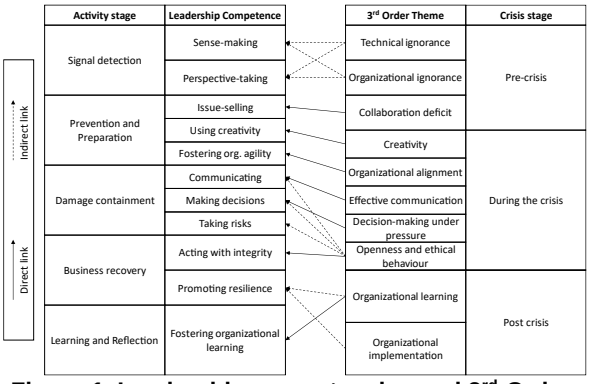

Figure 1. Leadership competencies and 3rd-Order themes

5.1. Signal Detection

In the first phase, signal detection, Wooten & James (2008) identify two leadership competencies: (a) sense-making and (b) perspective-taking. Sense making involves turning circumstances into a situation that is comprehended explicitly in words and that serves as a springboard into action, while perspective-taking consists in the ability to entertain or assume the perspective of another has been identified as a key element to social functioning. In the Norsk Hydro case, both of these competencies appear to be linked to two 3rd-order themes: technical ignorance and managerial ignorance. Evidently "ignorance" was the main factor contributing to the company's increased

exposure to the ransomware attack. In particular, it can be argued that on the one hand Hydro's leadership lacked perspective-taking capabilities before the crisis, which between 2017 and 2019 led to an important underestimation of the cyber risk to which the company was subjected. As a consequence of Hydro neglecting the importance of cybersecurity, the company didn't have adequate sense-making capabilities to avoid the attack or respond to it in a proactive manner. The shortcomings recorded in both competencies highlight the crucial role that cyber-risk-aware managers can play in signaling and preventing a cyber-related crisis from happening.

5.2. Prevention & Preparation

In the second phase, prevention and preparation, Wooten & James (2008) describe three competencies: (a) issue selling, the set of behaviors used by middle managers and employees to direct top management's attention to and understanding of important issues that otherwise would not be on their radar screen, (b) Organizational agility, the thorough knowledge of all aspects of how the business can work to accomplish a task, and (c) Creativity, the production of new or useful ideas, products, services, processes , or procedures. The first competence is closely related to the issue of collaboration deficit: the lack of communication between top management, middle management and company employees led to a situation where cyber awareness was poor at all levels in Norsk Hydro, thus nullifying one of the cornerstones of cyber crisis prevention. This highlights the crucial need for inter-actor collaboration and transparency to increase an organization's cybersecurity posture.

As for organizational agility and creativity, these are reflected in the 3rd-order themes organizational alignment and creativity. However, it is important to note that unlike in the Wooten & James model, where these two competencies are expected before the crisis is triggered, in the Norsk Hydro case the two are found to be useful also and above all during the crisis. This eventuality was foreseen by Wooten & James themselves, who pointed out that there is little evidence of the firms "*[…] displaying creativity during the preparation and planning stage"*. However, this does not undermine the importance of the two competencies. In the analysis it is mentioned several times how "creativity" was a vital factor enabling Hydro to manage the crisis. The same is true for organizational agility, which in this case was also reinforced by the existing organizational culture.

5.3. Damage Containment

In the third phase, Wooten & James (2008) identify three key competencies: (a) decision-making, described as the ability to make sound and rapid decisions under pressure, (b) effective communication, used to positively shape the stakeholders' perceptions of the crisis and the organization, (c) risk-taking, the willingness of assuming the risks of sharing information when experiencing a threat. The first two competencies are clearly found in the 3rd-order themes by the same name. In particular, the analysis shows that the ability to make important decisions under pressure proved fundamental to take the lead in the crisis, and that a large part of its resolution was due to independent-and bold decision-making by top and middle managers. The role of communication was even more important: from the analysis, it clearly appears that extensive internal and external communications were crucial in aiding Hydro during the attack. It is interesting to note how having a pre-established communications plan, another element that emerged as relevant from the narrative analysis, could be more related to a preliminary phase of the crisis, namely prevention and preparation. Finally, it was not possible to trace a precise connection between a 3rd-order theme and the risk-taking capability. However, this competency (and its importance) can be at least partially associated with some of the choices made by the company, such as that of communicating the event with the outside world in a transparent manner from the beginning of the crisis.

5.4. Business Recovery

Regarding business recovery, the two competencies highlighted by Wooten & James (2008) are (a) promoting organizational resiliency, the ability to return the organization to a precrisis state, and (b) acting with integrity, the ability to engage in ethical decision making and behavior. As for the first competence, there is no perfect parallel with a 3rd-order theme. However, moving towards resilience is something that can be indirectly connected to the themes of organizational learning and organizational implementation. With respect to acting with integrity, this is directly linked to the theme of openness and ethical behavior. As for previous examples, it is interesting to note 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.

5.5. Learning and Reflection

In the learning and reflection phase, Wooten & James (2008) describe only one competence: organizational learning, the capacity to go over the recovery phase thanks to post-crisis learning activities. This capability is perfectly evident in the homonymous 3rd-order theme. 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. Based on these two learning points, this study argues that the crisis established a future sense of direction for the company. Interestingly, one of the 3rd-order themes that it was not possible to completely trace back to any leadership competence envisaged by Wooten & James is organizational implementation. We argue that this 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.

6. Conclusions

Over the last few years, the pervasiveness of digital technologies led to a proportional growth in the number and severity of cybercrimes, with ransomware playing a very important role in this scenario. Despite the consequent increase in the number of cyber-related organizational crises, the literature on the subject is still lacking. The following paper aims to fill the research gap on the topic. In particular, by applying the Wooten & James model for crisis management leadership competencies to the case study of a company victim of a ransomware attack, the study provides interesting insights to understand which traditional leadership competencies can be more useful to face a cyber crisis.

From the study, it emerges that 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 case study also emphasizes the importance of issue-selling as a key competence to ensure awareness of cyber risks at the employee level, to establish a shared direction and create engagement around the topic.

Among the competencies necessary to properly handle the crisis, communication and the ability to make decisions under pressure were confirmed to be among the most important. The study also highlights 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. Furthermore, the study shows how two leadership competencies, creativity and organizational agility, 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.

The study also describes 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.

Finally, among the most important post-crisis leadership competencies, the study claims the relevance of a leadership competence absent in the Wooten & James model, namely that of implementing the learnings from the crisis. Organizational implementation is the step that can effectively lead to the creation of a cyber-resilient security culture that acts proactively and not reactively.

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 study adds to the literature by increasing the understanding of how organizations can manage cyber-related crises, ultimately contributing to help them moving towards cyber risk resilience.

6.1. Limitations

The main limitation of the present study is related to its data collection. This study is based on a single case study, wherein the data used is of secondary and qualitative nature. These limitations reveal the following suggestions. First, a deeper investigation into the present case study could be achieved by using primary data. This could reveal insights not captured in this study, such as the leadership style that characterized Norsk Hydro and how it affected the management of the crisis. Second, further research could investigate other case studies that display other characteristics (different geography, response, etc.). Finally, it could also be interesting to investigate the leadership competencies in other types of organizations such as governments, hospitals, and educational institutions. This could reveal additional elements not captured through the lens of companies.

7. References

Backman, S. (2021). Conceptualizing cyber crises. Journal of contingencies and crisis management, 29(4).

Batra, S., Gupta, M., Singh, J., Srivastava, D., & Aggarwal, I. (2020). An Empirical Study of Cybercrime and Its Preventions. In 2020 Sixth International Conference on Parallel, Distributed and Grid Computing. IEEE.

Bechler, C. (1995), "Looking beyond the immediate crisis response", Journal of the Association for Communication Administration, Vol. 1, pp. 1-17.

Bhaduri, R. M. (2019). Leveraging culture and leadership in crisis management. European Journal of Training and Development.

Bolman, L. C., & Deal, T. E. (1997). Refraining organizations. San Francisco: Jossey-Bass.

Brockner, J. B., & James, E. H. (2008). Toward an understanding of when executives see opportunity in crisis. Journal of Applied Behavioral Science, 44(7).

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

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

Connolly, L. Y., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape. Computers & Security, 87.

Coombs, W. (1999). Ongoing crisis communication: Planning, managing and responding. Sage.

Couburn, J. Daffron, A. Smith, J. Bordeau, É. Leverett, S. Sweeney, T., (2018) Cyber Risk Outlook 2018, University of Cambridge.

Denis, J., Lamothe, L., & Langley, A. (2001). The dynamics of collective leadership and strategic change in pluralistic organizations. Academy of Management Journal, 44(4), 809-837.

Dutton, J. E., & Jackson, S. E. (1987). Categorizing strategic issues: Links to organizational action. The Academy of Management Review, 12(1), 76-90.

ENISA (2014). Report on Cyber Crisis Cooperation and Management. ENISA.

Ferdinand, J. (2015). Building organisational cyber resilience. Journal of business continuity & emergency planning, 9(2), 185-195.

Goutam, R. K. (2015). Importance of cyber security. International Journal of Computer Applications, 111(7).

Hay, I. (2016). Qualitative research methods in human geography (Fourth edition). Oxford University Press.

Holla, K. Titko, M. & Ristjev, J., (2018) Crisis Management - Theory and Practise. IntechOpen.

Holt, T., & Bossler, A. (2015). Cybercrime in progress: Theory and prevention of technology-enabled offenses. Routledge.

Iansiti, M., & Lakhani, K. R. (2014). Digital ubiquity: How connections, sensors, and data are revolutionizing business. Harvard business review, 92(11), 19.

James, E. H., & Wooten, L. P. (2005). Leadership as (un)usual: How to display competence in times of crisis. Organizational Dynamics, 34(2), 141-152.

Leppanen, S., Ahmed, S. & Granqvist, R., (2019). Cybersecurity Incident Report: Norsk Hydro. Sciencedirect.

Loeb, L., (2019). Norsk Hydro: This is How you React to a Ransomware Breach. Dark Reading.

McIntosh, T., Kayes, A.S.M., Chen, Y.P., Ng, A. And Watters, P., (2022). Ransomware Mitigation in the Modern Era. ACM computing surveys, 54(9), pp. 1-36.

Mitroff, I., & Pearson, C. M. (1993). Crisis management: A diagnostic guide for improving your organization's crisis-preparedness. Jossey-Bass.

Moen, T. (2006). Reflections on the narrative research approach. International Journal of Qualitative Methods, 5(4), 56-69.

Mohammad, A.H., (2020). Ransomware Evolution, Growth and Recommendation for Detection. Modern applied science, 14(3), pp. 68.

Pearson, C., & Clair, J. (1998). Reframing crisis management. Academy of Management Review, 23(1).

Pheng, L., Ho, D., & Ann, Y. (1999). Crisis management: A survey of property development firms. Property Management, 17(3), 231-251.

Ponemon Institute (2021). Cost of a Data Breach Report.

Prevezianou, M. F. (2021). Beyond ones and zeros: Conceptualizing cyber crises. Risk, Hazards & Crisis in Public Policy, 12(1), 51-72.

Roux-Dufort, C., (2007). Is Crisis Management (Only) a Management of Exceptions?. Journal of Contingencies and Crisis Management, 15(2), pp.105-114.

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

Shaw, G., & Harrald, J. (2004). Identification of the core competencies required of executive level business crisis and continuity managers. Journal of Homeland Security and Emergency Management, 1(1), 3-18.

Sonicwall (2022). 2022 Sonicwall Cyber Threat Report.

Sophos (2021). The State of Ransomware 2021.

Sun, S. (2008), "Organizational culture and its themes", International Journal of Business and Management, 3(12).

Tidy, J., (2019). How a ransomware attack cost one firm £45m. BBC News. Available at: https://www.bbc.com/news/business-48661152

Wall, D. S. (2013). Criminalising cyberspace: The rise of the Internet as a 'crime problem. In Handbook of internet crime (pp. 88-103). Willan.

Wang, W., & Belardo, S. (2005). Strategic integration: A knowledge management approach to crisis management. Proceedings of the 38th HICSS.

Webster, L., & Mertova, P. (2007). Using narrative inquiry as a research method: An introduction to using critical event narrative analysis in research on learning and teaching. Routledge.

Wooten, L. P., & James, E. H. (2004). When firms fail to learn: The perpetuation of discrimination in the workplace. Journal of Management Inquiry, 13(1).

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.