INTRODUCTION

The outbreak of the COVID-19 pandemic crisis around the world and the resulting unprecedented measures taken by governments required organizations to quickly adopt new ways of (remotely) working. At face value, this would suggest a higher vulnerability for cyber threats. This research note analyses how a global financial institution dealt with this challenge by using Hollnagel's four abilities for resilient performance as a theoretical lens. Semi-structured in-depth interviews with eleven key actors were conducted. Three findings stand out. First, the interviews suggest that the organization performed cyber resiliently in the sense that the number of incidents and impact were not significantly higher. Second, the interviews show that all four abilities of resilience were formally developed prior to the COVID-19 outbreak, but rarely resulted in anticipatory adjustment. Third, the interviews indicate that the ability to respond contributed most to the organization's cyber resilience during the pandemic crisis. To conclude, our research note raises the question to what extent the four potentials should be developed beforehand in order to perform resiliently during crises.

KEYWORDS

corona, COVID-19, cyber, cyber security, resilience, threats, vulnerability

1 | INTRODUCTION

The outbreak of the COVID-19 pandemic crisis around the world and the resulting unprecedented measures taken by governments are having a significant impact on our society at large. Organizations were forced to quickly adopt new ways of remotely working, utilizing new systems for communication and altered practices to meet social distancing requirements and modified work patterns (Dwivedi et al., 2020; Herath & Herath, 2020; Wirth, 2020). The first studies on this indicate that the outbreak of COVID-19 have made organizations become more vulnerable to cyber threats. On the one hand, cyber threats and incidents have reported to rise as a result of a shift in crime opportunities from offline to online environments (Buil-Gil et al., 2020; Lallie et al., 2020). On the other hand, the sudden and rushed response to the pandemic crisis has created major cyber security gaps in organizations (Škiljić, 2020). Organizations were forced to quickly allow employees to work from home, without necessarily considering the cyber security implications on their ICT, employees and organization (Abukari & Bankas, 2020; Dwivedi et al., 2020; Wirth, 2020).

In this research note, we analyse how a global financial institution (GFI) dealt with this challenge. More specifically, we study how the pandemic crisis affected the ability of the GFI to remain cyber resilient, that is the ability of the organization to securely continue and adapt its required digital operations under both expected and unexpected conditions including adverse cyber events (c.f. Björck et al., 2015). According to Kott and Linkov (2021: 80) the key notion of cyber resilience is acceptance of cyber compromise as a likely event, and the organization suffers as a result; the focus is on the organization's ability to recover and adapt, and not just resist. Cyber resilience, the authors continue, characterizes what happens after an adverse event, and requires preparedness for both known and unknown threats. In our research we use Hollnagel's four potentials of resilient performance – that is, the potential to anticipate, monitor, respond and learn – as a theoretical lens. Our aim is to contribute to the current literature on cyber resilience, which, although quickly
emerging, contains relatively few empirical case studies (see e.g., Barasa et al., 2018 for resilience case studies in other sectors). In addition, our research adds to the emerging literature on the implications of a ‘black swan’ event for the cyber security of organizations.

This research note is organized as follows. First, we briefly discuss Hollnagel’s theory of resilience. Second, we give insight into the methodology of our research. Third, we present the findings which have been compressed in order to comply with the format of a re-search note. To conclude, we discuss the implications of our findings for theory and practice.

2 | HOLLNAGEL’S THEORY OF RESILIENCE

There are different viewpoints that can be used to study resilience (e.g., Hynes, Trump, Love, Kirman, et al., 2020; Hynes, Trump, Love, & Linkov, 2020; Groenendaal & Helsloot, 2020; Kott & Linkov, 2021). In our study, we decided to use the theory developed by Hollnagel (2011). The reason why we used this perspective in our research is threefold. First, Hollnagel’s view on resilience is widely accepted in the literature on organizational resilience and has previously been applied to the cyber security domain (e.g., Van der Kleij & Leukfeldt, 2019). Second, a major advantage of Hollnagel’s approach is that it provides a lens through which resilient performance can be observed and assessed. It should be noted here that researchers have only recently begun to investigate how resilience can be quantitatively measured (e.g., Kott & Linkov, 2021) and therefore we rely on qualitative approaches to measure cyber resilience. The third reason is that we discovered that elements of Hollnagel’s approach are being used in practice. As an example, the European Central Bank (ECB) has published guidance on cyber resilience for financial market infrastructures which includes several expectations regarding the development of the four potentials which can be traced back to the cyber resilience framework that the ECB is using (ECB, 2018).

In Hollnagel’s (2011, 2017) view, resilience is a characteristic of how an organization performs and not a quality that the organization as such possesses. According to Hollnagel (2017), resilient performance means that the organization is able to continue its required operations under both expected and unexpected conditions by adjusting its functions prior to, during or following certain events (e.g., changes, disturbances and opportunities).

The key characteristic of resilient performance is the ability of the organization to adjust how it functions. According to Hollnagel (2011, 2017), adjustments can be made either after something has happened (reactive, responding to feedback) or before something happens (anticipatory or proactive, directed by assumptions about the future). In practice, both types of adjustment are likely to be happening in organizations. Hollnagel (2017) stresses that reactive adjustments are most common, but do not guarantee the continuity of the organization. For instance, organizations that do not anticipate an economic downturn and operate with tight margins have few opportunities to cope with setbacks during a recession. Proactive adjustment implies that the system changes to meet future demands that are expected. This also includes changing from a state of normal operation to a state of heightened readiness before something happens (Hollnagel, 2017). In this state of heightened readiness, resources are allocated to match the needs of the expected event and special functions may be activated.

According to Hollnagel (2011) and others (Leveson, 2016; Woods, 2015), organizations need to develop four abilities that are required to achieve a resilient performance: the ability to anticipate, monitor, respond and learn.

- The ability to anticipate means being able to anticipate developments further into the future. This can be potential disruptions, new requirements, constraints or novel opportunities (Hollnagel, 2017). According to Chuang et al., (2020), the ability to look ahead and to consider future events, conditions, threats and opportunities is a competitive and (evolutionary) advantage.
- The ability to monitor considers how well the organization can detect changes to work conditions and the indicators used to keep track of what happens in the internal and external environment (Chuang et al., 2020). According to Hollnagel (2017), monitoring must cover an organization’s own performance as well as what happens in the operating (external) environment.
- The ability to respond entails knowing what to do and being able to timely and effectively respond to what happens (Hollnagel, 2017). This includes responding to regular and irregular changes, disruptions and opportunities by activating prepared actions, adjusting the current way of working and/or inventing new modes of operating (Chuang et al., 2020).
- The ability to learn means knowing what has happened and being able to learn from experience (Hollnagel, 2011). According to Hollnagel (2017), learning the right lessons from the right experience is key. This includes single-loop learning from specific experiences (i.e., trying to understand why certain objectives are not met) and double-loop learning (i.e., challenging the objectives themselves, seeking for the underlying causes) (Hollnagel, 2011; Chuang et al., 2020).

Importantly, Hollnagel (2017) recognizes that having developed the four potentials does not necessarily result in a resilient performance when needed for example during a crisis. He states that an organization that has developed them will be more likely to perform in a way that is resilient than one that has not. And an organization that completely lacks the potentials, he adds, will be incapable of resilient performance (Hollnagel, 2017).

3 | METHODOLOGY

Our research entails a case study of a GFI. The GFI provides financial (e.g. insurance) services and products to customers around the world. The GFI – and this applies more broadly to the entire financial sector – is rapidly transforming into a technology business. The vast majority of interaction between customers at the GFI is through digital channels. As a consequence, cyber security has become of strategic importance for this GFI.
The chief information security office led by the Chief Information Security Officer (CISO) is responsible for (amongst others) cyber and information security as well as digitalized fraud (e.g., phishing attack on customers in which the attacker impersonates the organization).

Semi-structured interviews with eleven respondents from the strategic, tactical and operational layer of the organization were conducted. Table 1 provides an overview of the respondents and their roles within the organization and the labels that are used in the results section when referring to the respondents. Admittedly, the total number of respondents is not large in absolute numbers. However, from a cyber security and digitalized fraud perspective, all of the respondents fulfill key positions within the organization which makes their view on the research topic very relevant and more reliable. To put it differently, if anyone in the organization could know the impact of the COVID-19 pandemic crisis on the cyber resilience of the organization, it should be the respondents selected for this study. Furthermore, the strategic, tactical and operational selection of respondents ensures that both the front line and policy perspective is captured (see also Groenendaal, 2015).

Interview questions were derived from examples formulated by Hollnagel (2017). The interviews took place between April and October 2020 and lasted for about 30–45 min on average. The key points and some illustrative quotes of the interviews were written down. Some of the respondents were interviewed twice, usually with some time (e.g., 2–3 weeks) between the interviews in order to follow up upon questions that came up afterwards.

4 | RESULTS

Based on the interviews, three observations can be drawn about how the GFI has dealt with the challenges arising from the COVID-19 pandemic crisis.

| Role of respondent | Label |
|-------------------|-------|
| **Strategic layer** | |
| #1 Deputy Chief Information Security Officer | DCISO |
| #2 Chief Cyber Security Operations | CCOPS |
| **Tactical layer** | |
| #3 Information Security Manager 1 | ISM1 |
| #4 Information Security Manager 2 | ISM2 |
| #5 Head of Incident Response | HIR |
| #6 Business Continuity Manager | BCM1 |
| **Operational layer** | |
| #7 Digital Fraud Investigator 1 | FI1 |
| #8 Digital Fraud Investigator 2 | FI2 |
| #9 Cyber Threat Analyst | CTA |
| #10 Cyber Intelligence Analyst 1 | CIA1 |
| #11 Cyber Intelligence Analyst 2 | CIA2 |

4.1 #1: Considering GFI’s incident statistics, the organization performed cyber resiliently during the crisis

The majority of respondents indicated that the organization has become more vulnerable to cyber threats during the outbreak of the COVID-19 pandemic crisis. ISM1 for instance mentioned that the swift implementation of working from home has led to a major increase of the attack surface. ISM2 noted that working from home resulted in less visibility on endpoints of employees, especially when they are not connected to the corporate network. As a consequence, the respondents note, the organization is more vulnerable to attacks that either uses the endpoint of employees as a stepping stone to penetrate the corporate network or to steal or manipulate data that is stored on that particular endpoint. In addition, FI1, FI2, CIA1, and CIA2 explained that major social events such as COVID-19 provide opportunities for cybercriminals to make phishing attacks more effective as people tend to be more inclined to believe the message of the phisher. Furthermore, CIA1, CIA2 and FIA1 emphasized that the organization has become more vulnerable to insider threats, that is employees with malicious intent. CIA1 explained that usually the majority of insider threats are detected thanks to vigilant colleagues close to the rogue employee. But employees with malicious intent working from home due to COVID-19 are less likely to get caught by other employees.

However, DCISO and CCOPS stressed that incident statistics show that these cyber threats have not materialized. Although the number of phishing attacks increased during the outbreak of COVID-19 and many phishing campaigns were related to the pandemic, the respondents indicated that the actual success rate and damage were only a little higher than average. Standard operating procedures were sufficient to handle these attacks. During the pandemic crisis, the GFI only faced slightly more cyber incidents than a year before. The pandemic crisis has not caused many problems in managing these incidents, also because cyber incident responders were used to work remotely from time to time before COVID-19. In a few cases, when the impact of incidents was (potentially) larger, DCISO, CCOPS and HIR decided to physically meet in the dedicated crisis control room, because physical meetings were perceived to be better for the communication and coordination between IT, security and business.

4.2 #2: All four abilities of resilience were developed prior to the crisis, but rarely resulted in anticipatory adjustment

Interviews with all respondents demonstrated that all the four abilities needed to perform resiliently were present to a certain extent prior to the pandemic crisis.

4.2.1 The ability to anticipate

The GFI has a dedicated cyber threat intelligence unit responsible for the development of a quarterly threat landscape report and the
daily gathering and analysis of cyber threat intelligence information. CIA1, CIA2 and DCISO indicated that the threats caused by the COVID-19 pandemic were not foreseen upfront and hence not covered in the quarterly threat landscapes. In addition, the GFI has a business continuity management (BCM) capability responsible for the development of an annual corporate threat report. According to BCM1, several internationally renowned sources such as the Business Continuity Institute (BCI) Horizon Scan Reports and the World Economic Forum (WEF) Global Risks Reports were used in the development of these corporate threat reports. However, as noted by respondents, none of the corporate threat reports of the past 5 years mentioned the threat of a major infectious disease outbreak including stringent governmental lockdowns. BCM1 indicated that some business units and departments within the GFI had an infectious disease plan available that focused upon sick leave of its own staff and the deployment of basic hygiene measures. However, these plans were considered to be inapt for the corona crisis as they did not take into account the draconic measures of the government.

4.2.2 | The ability to monitor

DCISO and CCOPS showed that the organization has invested in internal reporting on cyber threats and incidents. Key performance indicators have been established and agreed upon by senior management and used on a daily, weekly or monthly basis to inform operational, tactical and strategic decision-makers. In addition to the reporting by the CISO department, there is also the IT risk department that has a separate reporting line on IT security risks to senior management and regulatory supervisors.

4.2.3 | The ability to respond

The GFI has several incident management capabilities developed. For cyber incidents, the GFI has an extensive cyber incident response capability (Security Operations Center) which operates 24/7 according to a follow-the-sun principle. The cyber incident response capability works closely together with the IT incident management organization, which is responsible for responding to IT failures that result in business impact. In case of a major cyber security incident, this IT incident management capability can be used to quickly deploy changes (e.g. patch vulnerable systems, change configuration settings, implement workarounds) within the IT environment. Furthermore, the GFI has developed a BCM capability that is responsible for ensuring that the organization can continue the delivery of services in case of a business disruption. According to BCM1, a quick recovery of services following disruption is ensured by having contingency plans in place and a crisis management organization available to facilitate rapid decision making by senior management.

4.2.4 | The ability to learn

According to HIR, the majority of cyber incidents are evaluated during cyber incident response team meetings. In addition, for larger incidents there is a formal incident learning process established which includes an evaluation session with all stakeholders involved and the development of lessons learned including root cause analysis and action plan requiring approval from senior management. BCM1 indicated that some departments and entities had gained experience with previous infectious diseases such as the swine flu (2009). According to BCM1, these experiences have been recorded in at least some of the available pandemic plans. Finally, no respondent could give a concrete example of organizational adjustment in anticipation of the pandemic crisis. Interviews demonstrated a reactive response of the GFI to the unfolding situation. DCISO and BCM1 pointed out that the GFI has started monitoring the pandemic outbreak in China at an early stage (mid-January 2020). Daily calls were organized to exchange information about the pandemic. However, these calls have not led to proactive actions except imposing travel restrictions to infected countries. For instance, only after the first infections were reported and it became clear that soon all surrounding countries would be impacted, it was decided to centrally consider the available pandemic plans, which then appeared to be outdated or not usable. As another example, DCISO mentioned that the expansion of remote connections and its cyber security was only seriously considered after governments imposed lock-downs.

4.3 | #3: The ability to respond contributed most the GFI’s resilient performance during the crisis

DCISO, CCOPS, HIR, ISM1, ISM2 and BCM1 were able to provide several examples showing that the GFI – albeit reactive – has responded well to the pandemic crisis. The main example is the massive extension of the working from home capacity. DCISO, ISM1 and IS2 indicated that within a few weeks, infrastructure and processes have been transformed to enable the vast majority of the workforce to work from home securely. According to DCISO, this was an unprecedented success for a large company partly made possible because of its own mature IT and security capabilities as well as good relationships (and contracts) with third party suppliers. Respondents also provided some examples of the abilities of anticipation and monitoring, but these examples all occurred once the organization was already in crisis (and thus response) mode. For instance, CCOPS and HIR stressed that the primary cyber security services were never interrupted or constrained by the outbreak of the crisis. According to these respondents, this was partly due to anticipatory adjustments such as implementing fixed teams to contain the potential spreading of the coronavirus within the team. As another example, FI1 and FI2 noted that a special task force was established to monitor certain fraud threats targeting the organization and/or
customers. According to them, this helped to take swift actions following attacks, such as adjusting e-mail configuration settings and initiating targeted awareness campaigns.

5 | DISCUSSION

In this research note, we briefly analysed how a GFI dealt with the challenges posed by the COVID-19 pandemic crisis by using Hollnagel’s four abilities for a resilient performance as a theoretical lens. Although the pandemic crisis has made the GFI more vulnerable to certain cyber threats, the results of our tentative investigation show that the organization performed resiliently considering the incident statistics and the fact that the organization has responded well to the challenges posed by the pandemic crisis – albeit reactively.

Our findings may shed a different light on Hollnagel’s theory of resilience. First, our case study indicated that three out of four abilities (i.e., anticipate, monitor and learn) seem to explain little about the cyber-resilient performance of the organization. This raises the question to what extent the four abilities need to be developed in order to be able to perform resiliently. Second, we found examples of monitoring and anticipation, but these examples all relate to the moment when the organization was in crisis mode and hence could be regarded as (ability to) response activities too.

The importance of the ability to respond and particularly having the means (i.e., resources) to respond is highlighted in previous research as well. Based on a review of the empirical literature on organizational resilience, Barasa et al., (2018) found that the availability of resources is considered a key enabler of organizational resilience. When material resources are used strategically, the authors state, organizations can overcome disruption. The authors emphasize that financial resources are also considered necessary to mobilize other needed resources during the crisis. In a similar vein, what we have uncovered in this case reflects an analogy for companies of a well-known fact when it comes to resilience of individuals; in the end, having money at hand to be able to respond is a factor of greater importance than having put much effort in preparation (Helsloot & Ruitenberg, 2004).

Furthermore, we agree with Kott and Linkov (2021) that more scholarly effort should be devoted to resilience measurement. For instance, based on their definition of resilience (“cyber resilience refers to the system’s ability to recover or regenerate its performance after cyber-attacks produces a degradation of its performance”, Linkov & Kott, 2019:5), cyber resilience can only be measured in case of an attack that significantly impacted the organizational performance. As we did not come across any example of a cyber incident that led to major performance degradation (which also need to be defined and measured), the question can be raised what conclusions about the cyber resilience of the organization can be drawn in this specific case study.

Finally, a limitation of our study is our research design that does not make it possible to generalize the results of our research. Consequently, we call for more (comparative) case study research on cyber resilience in general and specifically in the context of adverse events such as major cyber-attacks or COVID-19. To conclude, it should be noted here that our tentative investigation only spans the first year of the pandemic crisis, and as the crisis still continues, we recommend researchers to conduct more extensive investigations to understand how cyber resilience of organizations evolve over time. Should further research, both quantitatively and qualitatively, along the line of this research note come up with similar findings then the formal expectations of for example the ECB that asks for the development of all four potentials come into question.

ENDNOTE

1 There is a debate in the literature whether the outbreak of COVID-19 pandemic crisis should be considered as a black swan. We hold the opinion that not the pandemic itself but the governmental response to it should be seen as such.

REFERENCES

Abukari, A. M., & Bankas, E. K. (2020). Some cyber security hygienic protocols for teleworkers in COVID-19 pandemic period and beyond. *International Journal of Scientific & Engineering Research, 11*(4), 1401-1407.

Barasa, E., Mbau, R., & Gilson, L. (2018). What is resilience and how can it be nurtured? A systematic review of empirical literature on organizational resilience. *International Journal of Health Policy and Management, 7*(6), 491-503. https://doi.org/10.15171/ijhpm.2018.06

Björck, F., Henkel, M., Stina, J., & Zdravkovic, J. (2015). Cyber resilience—fundamentals for a definition. In Rocha, A., Correia A., Costanzo S., Reis L., *New contributions in information systems and technologies*. Advances in Intelligent Systems and Computing 353. Springer, Cham. https://doi.org/10.1007/978-3-319-16486-1_31

Bui-Gil, D., Miro-Llinares, F., Moneva, A., Kemp, S., & Diaz-Castaño, N. (2020). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies, 23*, 547-559. https://doi.org/10.1080/14616696.2020.1804973.

Chuang, S., Ou, J. C., Hollnagel, E., & Hou, S. K. (2020). Measurement of resilience potential-development of a resilience assessment grid for emergency departments. *PLoS One, 15*(9), e0239472. https://doi.org/10.1371/journal.pone.0239472

Dwivedi, Y. K., Hughes, D. L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J. S., Gupta, B., Lal, B., Misra, S., Prashant, P., Raman, R., Rana, N. P., Sharma, S. K., & Upadhyay, N. (2020). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *International Journal of Information Management, 55*, 102211. https://doi.org/10.1016/j.ijinfomgt.2020.102211

European Central Bank (ECB) (2018). *Cyber resilience oversight expectations for financial market institutions*. ECB.

Groenendaal, J. (2015). *Frontline command: Reflections on practice and research*. Eleven International Publishing.

Groenendaal, J., & Helsloot, I. (2020). Organisational resilience: Shifting from planning-driven business continuity management to anticipated improvisation. *Journal of Business Continuity & Emergency Planning, 14*(2), 102–109.

Helsloot, I., & Ruitenberg, A. (2004). Citizen response to disasters: A survey of literature and some practical implications. *Journal of Contingencies and Crisis Management, 12*(3), 98–111. https://doi.org/10.1111/j.0966-0879.2004.00440.x

Herath, T., & Hemantha, S. B. (2020). Coping with the New Normal Imposed by the COVID-19 Pandemic: Lessons for technology management and governance. *Information Systems
Hollnagel, E. (2011). RAG: The resilience analysis grid. In Resilience engineering in practice. A guidebook. Farnham, UK: Ashgate.
Hollnagel, E. (2017). Safety-II in practice: Developing the resilience potentials. Taylor & Francis.
Hynes, W., Trump, B. D., Love, P., Kirman, A., Galaitsi, S. E., Ramos, G., & Linkov, I. (2020). Resilient financial systems can soften the next global financial crisis. Challenge, 63(6), 311–318. https://doi.org/10.1080/05775132.2020.1822660
Hynes, W., Trump, B., Love, P., & Linkov, I. (2020). Bouncing forward: A resilience approach to dealing with COVID-19 and future systemic shocks. Environment Systems and Decisions, 40, 174–184.
Kott, A., & Linkov, I. (2021). To improve cyber resilience, measure it. arXiv preprint arXiv:2102.09455.
Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2020). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. arXiv preprint arXiv:2006.11929.
Leveson, N. G. (2016). Engineering a safer world: Systems thinking applied to safety (p. 560). The MIT Press.
Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. In Kott A., Linkov I., Cyber resilience of systems and networks. Risk, Systems and Decisions. Springer, Cham. https://doi.org/10.1007/978-3-319-77492-3_1.
Škiljić, A. (2020). Cybersecurity and remote working: Croatia’s (non-) response to increased cyber threats. International Cybersecurity Law Review, 1(1), 51–61. https://doi.org/10.1365/s43439-020-00014-3
Van der Kleij, R., & Leukfeldt, R. (2019). Cyber resilient behavior: Integrating human behavioral models and resilience engineering capabilities into cyber security. In International conference on applied human factors and ergonomics (pp. 16–27).
Wirth, A. (2020). Cyberinsights: COVID-19 and what it means for cybersecurity. Biomedical Instrumentation & Technology, 54(3), 216–219. https://doi.org/10.2345/0899-8205-54.3.216
Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. Reliability Engineering & System Safety, 141, 5–9. https://doi.org/10.1016/j.ress.2015.03.018

How to cite this article: Groenendaal J, Helsloot I. Cyber resilience during the COVID-19 pandemic crisis: A case study. J Contingencies and Crisis Management. 2021:00:1–6.
https://doi.org/10.1111/1468-5973.12360