THE HAGUE
UNIVERSITY OF
APPLIED SCIENCES

Kenniscentrum Cybersecurity
Lectoraat Risk Management & Cybersecurity
Jelle Groenendaal
j.groenendaal@hhs.nl
12 november 2020

Cyber crises require anticipation and improvisation

The ransomware attack on Maastricht University (2019) and the wiperware attack on Maersk (2017) painfully demonstrated that major incidents cannot be prevented and can even turn into cyber crises. The extent to which organisations can limit the impact of cyber crises is determined, among other things, by their business continuity and crisis management. How do you adequately organise these control measures, however? The new Risk Management and Cybersecurity Research Group at The Hague University of Applied Sciences will investigate these and other questions at the intersection of risk management and cybersecurity over the next four years. In this article, we give a first reflection based on several scientific insights.

A cyber crisis threatens the survival, integrity and/or reputation of an organisation

The malware attack on Maastricht University and the wiperware attack on the shipping and transport giant Maersk irrefutably clarified that cyber incidents can have such an impact on business operations that they can be considered cyber crises: failures, disruptions or misuses of information technology (IT) systems and/or services that threaten the survival, integrity and/or reputation of organisations and where decisions have to be made under (the perception of) time pressure and uncertainty. In the worst cases, cyber crises can even disruptive societal processes. For instance, due to the cyber-attack on Maersk, the APM Terminals in Rotterdam were completely out of service, forcing ships to divert and trucks to cause a traffic jam in the port and on highways [1].

Business continuity management (BCM) and crisis management can limit the impact

The cyber resilience of organisations is determined by their ability to prevent cyber incidents and, if they occur, to limit their impact. Parties such as the Dutch National Cyber Security Centre argue that major cyber incidents cannot be prevented [2], so organisations must focus on taking measures to manage their impact. Business continuity management (BCM) and crisis management are two such control measures. BCM is the process of controlling threats that can lead to disruptions that disable delivering products or services at acceptable, predetermined levels [3]. To this end, threats to the most important organisational processes are assessed and plans to guarantee continuity are determined in the event of a disruption. This is described in a so-called business continuity plan, which describes what to do in several threat scenarios, such as what to do if a critical IT system breaks down due to a patch or if an office building is unavailable due to fire. Crisis management is the ability of organisations to prepare for, respond to and recover from a (cyber) crisis [3]. Crisis management enters the picture when the business continuity plan is inadequate to the situation at hand. The current coronavirus crisis is a striking example: many organisations had not considered a lock-down and, with it, the need to allow large parts of the workforce to work from home. In that case, a crisis-management team can decide to expand the capacity to work at home and to facilitate working from home.

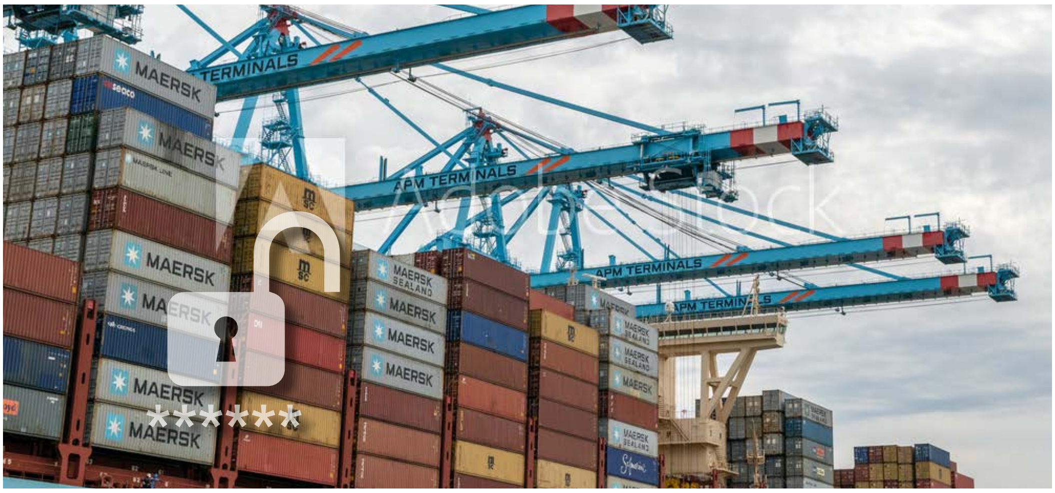
Limited empirical knowledge base necessitates research into BCM and crisis management

Much of the knowledge used to design, govern and organise information security comes from (international) standards. This also applies to BCM and crisis management, such as the ISO 22301 or BCI Good Practice Guidelines for BCM and the BS 11200 or TS 17091 for crisis management. These standards are used by many organisations worldwide and were developed by professionals who often have extensive experience in the field. Not much research has been conducted yet on the operations and effectiveness of these standards, and to date, implementing them has not been shown to lead to greater continuity or better managed (cyber) crises. Empirical research within organisations on the functioning and effectiveness of BCM and cyber crisis management is scarce. Applied research is therefore necessary to determine to what extent and how organisations can adequately prepare and respond to cyber crises.

BCM helps organisations anticipate predictable risks

The fact that little applied research actually exists on the operation and effectiveness of BCM and cyber crisis management within organisations does not alter the fact that several preliminary observations can be made based on existing research, examples of which we explore below.

The *first* finding is that BCM is theoretically suitable mainly for predictable risks [4]. BCM is based on classical management thinking (reductionism), which assumes that the world and therefore organisations are predictable and (therefore) manageable to a large extent. The BCM tools are therefore aimed at mapping organisational processes and (identifiable) risks and then taking measures to help guarantee continuity if they suddenly manifest. Examples of these predictable risks are office buildings that temporarily cannot be used due to fire or a payment system not functioning due to a server failing.



Anticipating on cyber crisis

BCM can be useful to prepare organisations for scenarios in which products or services can be temporarily undelivered or tardy due to a cyber incident. For example, a scenario can be drawn up for what to do in the event of a large-scale ransomware infection or DDoS attack. A few remarks must be made. First, it should be kept in mind that many business continuity plans contain actions based on the assumption that the network and regular means of communication, such as e-mail and telephones, will remain available during a disruption. Maersk has shown that a cyber incident can lead to a complete failure of IT networks and systems, so e-mail and telephony (which are dependent on networks) can no longer be used, preventing most plans from being carried out. The same thing could happen when a network is compromised, making communication unreliable. Second, building on the previous point, many business continuity plans are digitally stored and therefore cannot be accessed in the event of a network failure. Third, the risk that backups can be infected with malicious software that, for example, remains silent for a few months may prevent returning to a clean version. Fourth, with major ransomware infection, the burden on the IT organisation to clean and restore many workstations must be considered.

The second finding is that the planned responses that characterise BCM can only be effective if they are regularly practiced and performed [5]. The consequence of this finding is twofold. First, it means that BCM is especially suitable for (smaller) risks that regularly manifest themselves so that a feedback loop can arise between the plan and its implementation and plans do not degenerate into "paper tigers". Second, it means that BCM can only focus on a few risks because the time required to test plans is limited. A good BCM organisation therefore limits itself to the most common (recognisable) risks and ensures that insights from tests, exercises and real incidents are anchored in the plans and staff training.

BCM is less suited to a rapidly changing environment

However, BCM also has several limitations. The *third* finding is that BCM is less suitable for organisational environments that are subject to change. BCM places a great deal of emphasis on documenting organisational processes and establishing a response strategy that fits how the organisation is described on paper. In practice, however, this description is often not up to date when a disruption occurs. For example, IT systems may be phased out, new systems taken into production or certain key persons no longer employed due to a reorganisation or a replaced supplier. Although a business continuity management system (BCMS) generally states that plans should be revised annually or more frequently in the event of major changes, common organisational practice seems more unruly [4]. Some organisations and their environments are so subject to change that keeping an in-depth, up-to-date view of all critical processes at all times is impossible. In such environments, BCM often lags behind.

BCM does not get along very well with black swans

In addition to the predictable minor risks, several threats cannot be identified in advance. Donald Rumsfeld called these "unknown unknowns", or impactful, unpredictable events that are beyond the scope of risk management and thus BCM by definition. The *fourth* finding, then, is that BCM does not get along well with what Nassim Nicholas Taleb calls "black swans".

A first step of BCM is to identify threats and determine the extent to which they pose risks to the organisation. However, large, impactful events cannot always be predicted adequately. The current coronavirus crisis shows this beautifully. Flu pandemics occur every few years, but the current global response, with large-scale lockdowns and travel restrictions, has never been seen before. In the last five annual reports of the Global Risk Report of the World Economic Forum (WEF) – an important source of risk managers – infectious disease was not in the top 10 most likely major risks. In the latest 2020 edition of the report, infectious disease dangled at the bottom of the list of risks with the greatest impact. Interestingly, COVID-19 does not appear at all in the report published on January 15, 2020 [6].

Another important limitation of planned responses is that they offer little guidance when reality differs from that described in the plan. If during a cyber-attack, the systems are down for much longer than expected or unexpected cascade effects occur, the organisation must understand the problem on the spot and determine and implement a response strategy. This is the domain of (cyber) crisis management.

Crisis management helps organisations improvise

Crisis management helps organisations quickly bring expertise and mandates together to create environments for making meaningful decisions. Crisis management usually takes place on three levels: operational (e.g. in the SOC or CIRT), tactical (the head of CIRT) and strategic (CISO) [7].

Although hardly any research has been conducted on *cyber* crisis management, several conclusions can be drawn on the basis of the literature on crisis management.

First, all the research shows that professionals fall back on routine behaviour in crisis circumstances and therefore do what they have always done [5]. An important recommendation is therefore to align the (cyber) crisis organisation as much as possible with the regular organisation and not to expect or demand counterintuitive actions from people during crises. The fact that people fall back on ingrained habits during crises explains why evaluations often show that crisis plans are hardly consulted in the acute phases of crises (if at all). The value of such plans is therefore mainly in the "pre-crisis" phase: during preparation, they make experts and management aware of their roles, tasks and responsibilities during a cyber crisis.

Second, the literature shows that improvisation is inevitable during crises [8]. In some cases, employees will not have built up a routine for the situation before them or their routine simply does not work. At Maersk, for example, various forms of improvisation were visible: due to a lack of IT, the organisation booked new orders via WhatsApp and Gmail, devised an offline system to label containers and, within a few weeks, set up a completely new IT network [9].

Improvisation can bear a negative connotation. To some, it suggests that the organisation could have been better prepared for a particular disruption. In the scientific literature, however, improvisation is viewed in a much more nuanced way: as a necessary skill for people and organisations to respond adequately to unexpected opportunities and threats [10]. It is a misconception that improvisation does not require preparation. The scientific literature often uses the analogy of a jazz pianist, who can only improvise – that is, deviate from the standard – once they master the standard down to the finest detail [10]. In the context of crisis management, this can mean, for example, that crisis-management teams regularly practice "standard" crisis scenarios but also deviations from them. Strategic crisis-management teams should also learn that many decisions during crises are made by frontline professionals (e.g. cyber-incident responders) and how to facilitate their decision-making and adjust it where necessary.

Under crisis circumstances, professionals are susceptible to decision-making pitfalls

(Cyber) crises are characterised by time pressure, uncertainty and the major interests at stake. A third conclusion is that the literature finds professionals in these circumstances making mostly adequate decisions but also being prone to decision-making pitfalls [5]. These pitfalls apply at every level – operational, tactical and strategic – although they sometimes manifest in different ways. Their significance for cyber crisis management in practice is that crisis managers must be aware of them in their own decision-making and that of their subordinates. Common pitfalls include confirmation bias (the tendency to confirm an initial hypothesis by interpreting all received information in its light and only seeking evidence that supports it) and the sunk cost fallacy (the tendency to complete a task approaching the final phase simply because of the time and resources already sunk into it). These biases can occur, for example, when CIRT members investigate a certain hypothesis about a major incident for too long. Cyber crisis managers (in this case, the CIRT leader) must recognise these pitfalls and help members avoid them.

To conclude, more applied research is needed on BCM and cyber crisis management

In this article, we have described BCM and cyber crisis–management insights based on the scientific literature. According to the literature, anyone seeking to limit the impact of cyber crises should focus on anticipation (BCM) and improvisation, which can be facilitated and adjusted with the help of crisis management. However, many questions remain unanswered, and more applied research is needed, such as the following: What do effective BCM and cyber crisis-management exercises look like? What does a robust cyber crisis–management organisation look like? How can you intelligently automate BCM without conceding effectiveness? To what extent do decision-making models help avoid decision-making pitfalls by cyber crisis–management teams? What is the role of the CISO in crisis management? The Risk Management and Cybersecurity Research Group hopes to investigate these and other questions with professionals in the field in the coming years.

Literature

1. Van Duin, M., & Maan, J. (2018). Cyberaanval op Maersk. *Lessen uit crises en mini-crises 2017*. Instituut Fysieke Veiligheid: Arnhem.
2. NCTV. (2020). Cybersecuritybeeld Nederland 2020.
3. NVN-CEN/TS 17091. (2018). Crisismanagement – Handreiking voor het ontwikkelen van strategisch vermogen.
4. Groenendaal, J., & Helsloot, I. (in press). Organizational resilience: Shifting from a planning-driven business continuity management to anticipated improvisation. *Journal of Business Continuity & Emergency Management*.
5. Groenendaal, J., & Helsloot, I. (2016). The application of naturalistic decision making (NDM) and other research: Lessons for frontline commanders. *Journal of Management and Organization*, 22(2), 173.
6. Van der Linden, L. (2020). Wat kunnen we met risicomanagement leren van virusinfecties die al dan niet uitgroeien van een pandemie. *Genootschap voor Risicomanagement*.
7. Groenendaal, J., Helsloot, I., & Scholtens, A. (2013). A critical examination of the assumptions regarding centralized coordination in large-scale emergency situations. *Journal of Homeland Security and Emergency Management,* 10(1), 113–115.
8. Greenberg, A. (2018, August 22). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
9. Mendonca, D., & Wallace, W. A. (2004). Studying organizationally situated improvisation in response to extreme events. *International Journal of Mass Emergencies and Disasters*, 22(2), 5–30.
10. Weick, K. E. (1998). Introductory essay – Improvisation as a mindset for organizational analysis. *Organization Science*, 9(5), 543.