Towards More Insight into Cyber Incident Response Decision Making and its Implications for Cyber Crisis Management

Jelle Groenendaal
Crisislab, The Netherlands
j.groenendaal@crisislab.nl

Ira Helsloot
Crisislab, The Netherlands
i.helsloot@crisislab.nl

Christian Reuter
Science and Technology for Peace and Security (PEASEC), TU Darmstadt
reuter@peasec.tu-darmstadt.de

ABSTRACT

Organizations affected by a cyber-attack usually rely on external Cyber Incident Response (CIR) consultants to conduct investigations and mitigate the impact. These CIR consultants need to make critical decisions that could have major impact on their clients. This preliminary investigation aims to get a better understanding of CIR decision -making and answers the following questions: (1.) To what extent do experienced CIR consultants use a Recognition-Primed Decision (RPD) Making strategy during their work? (2.) What are the implications for cyber crisis management as well as for training and decision -making? To answer these questions, we conducted a literature review and interviewed six experienced CIR consultants using the Critical Decision Method. Our analysis reveals that CIR consultants recognize situations based on past experiences and apply a course of action that has worked effectively in the past. This course of action is mainly aimed at collecting and evaluating more data. This finding differs from other operational domains, such as the military and fire department, where recognition is usually followed immediately by action. For cyber crisis management, this means that crisis management teams should decide to what extent and in what ways they want to mitigate the risk of responding belatedly to cyber events, which could potentially lead to unnecessary data theft and sustained business disruption. Another implication is that crisis management teams should consider whether additional forensic investigations outweigh the expected benefits throughout the response process. For instance, if the likely entry-point of the attacker has been discovered, how much effort should be devoted to exclude other potential entry-points. Reflecting on the status-quo, several implications for training and decision making are provided.

Keywords

Cyber Incident Response, Cyber Crisis Management, Naturalistic Decision-making

INTRODUCTION

Research and practice increasingly recognize that cyber incidents can not be completely prevented. Therefore, organizations must be prepared to deal with potential breaches. This recognition is captured in the concept of cyber resilience. Cyber resilience starts with accepting cyber compromise as a likely event with the organization suffering as a result (Kott & Linkov, 2021). Cyber resilience then focusses on the ability to make sense of what happens after an adverse cyber event and on the preparedness to handle both known and unknown results of such a breach (Kott & Linkov, 2021). Contrary to cybersecurity that focusses on the prevention of an attack, cyber resilience thus puts the focus on the organization's ability to absorb, recover and adapt (ibid). In short, cyber resilience puts emphasis on the ability of organizations to timely and appropriately respond to adverse cyber incidents (Groenendaal & Helsloot, 2021).

One key element of cyber resilience is Cyber Incident Response (CIR). The term refers to the reaction and associated measures in *direct* response to an IT security incident. It aims to detect the occurrence of an incident, contain the impact of the incident as much as possible, and eliminate the threat posed to the organization (Ahmad et al. 2021). Large organizations have their own CIR capabilities in diverse configurations. These large organizations commonly have a dedicated CIR capability consisting of a Security Operations Center (SOC), which can be outsourced or commissioned to continuously monitor, investigate, and respond to cyber threats and

incidents. In some of these organizations, the SOC is complemented with a Computer or Cyber Incident Response Team (CIRT), which provides additional technical expertise for threat analysis and incident response (Ahmad et al. 2021). Nowadays, Computer Emergency Response Teams (CERTs) are deployed in many countries and organizations. In Germany, CERTs in the public sector operate on the federal and state level to provide information security services for authorities, citizens, and enterprises (Riebe et al. 2021). Small to medium sized organizations usually do not have a dedicated CIR capability themselves. In these organizations, CIR is organized on an ad-hoc basis and could potentially be carried out by the IT manager, a rather small group within the IT unit, or an outsourced IT service provider (cf. Ebbers et al. 2020).

However, for most organizations it is found that in case of a major cyber incident existing CIR capabilities will not be sufficient. Therefore, most organizations rely on external (commercial) CIR service providers to assist them. External CIR service providers offer services to organizations that need immediate assistance in analyzing (e.g. determining root causes), mitigation (e.g. preventing further damage), remediating (e.g. removing the threat from the environment), and recovering (e.g. recovering lost information and reducing future vulnerabilities) from suspected or confirmed cyber incidents. Organizations can proactively hire CIR service providers in anticipation of potential attacks (e.g. through a contract which could give a discount and guaranteed support) or contact them as soon as they become aware of a (potential) cyber incident.

CIR service providers generally employ highly skilled and experienced CIR consultants focusing on forensic analysis, reverse malware engineering, threat investigation, and incident coordination, amongst others. Since these CIR consultants are involved in incident response activities on a daily basis and have gained experience in numerous different organizations, they are the most experienced professionals in their field. Consequently, much can be learned from the way these experienced professionals make decisions under challenging conditions. This preliminary research is a first attempt to gain insight into how experienced external CIR consultants make decisions, and to draw implications for cyber crisis management, as well as training and decision making.

In general, CIR consultants operate in a dynamic and constantly changing environment in which they need to actively engage in information management and problem solving while adapting to complex circumstances (Steinke et al. 2015). In this challenging environment, external CIR consultants are required to make critical decisions regarding the advice they should give to clients that are affected by a major cyber incident. They advise clients, for instance, whether or not a ransom should be paid in case of a ransomware attack. Additionally, they determine when an attacker needs to be removed from the IT network and advise their clients accordingly. The consequences of these decisions may be severe, and the decision making process is typically characterized by time pressure and uncertainty. Consequently, effective decision making is extremely difficult, but at the same time crucial in order to minimize the impact of the cyber incident on the customer (Van der Kleij et al. 2022).

Despite its relevance, CIR decision making has so far been an understudied topic. Previous research such as Ahmad et al. (2021) and Bartnes et al. (2016) has focused primarily on organization and management aspects of cyber incident response. Far less scholarly attention has been paid to the way cyber incident responders, individually and as a team, assess information and make decisions during their emergency response tasks. Consequently, CIR decision making deserves more research attention, as it is widely acknowledged in the academic literature that effective cyber incident response requires both professional incident responders and teams to take adequate decisions based on sufficiently developed situational understanding of the complex and evolving socio-technical environment (Ahmad et al. 2021).

The study of CIR decision making shows parallels with operational command in other domains. Much research has already examined the way in which experts make operational decisions under challenging conditions. This research relates to so-called naturalistic decision making, or NDM. According to Zsambok & Klein (1997: 5), NDM research examines how experienced people, working as individuals or in groups, react in dynamic, uncertain, and often fast-paced environments, identify and assess their situation, make decisions, and take actions based on consequences that impact themselves and the organization in which they operate. Recognition-primed decision making (RPD) is one of the most prominent models of NDM. It assumes that when under time-pressure, experienced decision makers recognize the situation based on a few indicators and apply a course of action that has worked before. RPD has been researched in various operational domains, including military, fire service, police, emergency health care, and aviation, but not within a CIR context.

Aiming to address the identified research gap, this preliminary research investigates RPD within a CIR context and will answer the following 2 questions:

1. *To what extent do experienced CIR consultants apply RPD during their work?*

2. *What are the implications for cyber crisis management as well as for training and decision-aiding?*

This paper is structured as follows. In the next section we will give a brief overview of the relevant literature on the CIR process, CIR decision making, and NDM. Then we will describe our empirical research methodology followed by the empirical findings of our research. We will conclude with the implications of our research for cyber crisis management and CIR decision making training and support.

LITERATURE REVIEW

CIR Process

This cyber incident response process aims to mitigate a potential threat, eradicate changes in the environment made by the adversary, remove the adversary from the environment, and restore normal operations. In general, it mainly consists of three main activities (Freiling & Schwittay, 2007):

1. *Initial response*: The main objectives of this step include assembling the response team, communicating with the client, reviewing network-based and other readily available data, determining the type of incident, and assessing the potential impact. The overall goal is to gather enough initial information to enable the team to identify an appropriate response.
2. *Investigation*: The main purposes in this step are to determine the facts that describe what happened, how it happened and, in some cases, who was responsible.
3. *Remediation*: The main objective in this step is to deploy remediation plans which considers factors from all aspects related to the situation, including legal, business, political, and technical aspects

In practice, several models exist to rely on when developing an incident response plan. The National Institute of Standards and Technology has released a Special Publication 800-61 Rev. 2, the 'Computer Security Incident Handling Guide' to provide an overview of the incident response process. Their model (shown in Figure 1) consists of four primary phases: Preparation, Detection and Analysis, Containment, Eradication, Recovery, and Post-Incident Activity (Cichonski et al, 2012).

Previous Research on CIR

As already mentioned before, cyber incident response remains an understudied area of research. Previous research has primarily focused on organization and management aspects of cyber incident response. Ahmad et al. (2021), for instance, conducted a single-case study to investigate the role of management practice in developing situation awareness of cybersecurity incidents. The authors developed a process model that explains how organizations can practice situation awareness of the cyberthreat landscape and the broad business context in incident response. In another study, Baskerville et al. (2014) used a comparative case study design to examine the strategic balance between prevention and response. The authors designed an overarching security framework that focuses on managing the proper balance between these two approaches. Moreover, Ahmad et al. (2012) conducted an exploratory in-depth case study to examine deficiencies in the practice of incident response. The case study revealed that incident response practices, in accordance with detailed best-practice guidelines, tend to have a narrow technical focus aimed at maintaining business continuity whilst neglecting strategic security concerns. The study also discovered that the limited post-incident follow-up process focused on 'high-impact' incidents rather than 'high-learning' incidents and 'near misses'. In another study, Ahmad et al. (2020) draw on organizational learning theory to develop a conceptual framework that explains how information security management and incident response functions may create learning opportunities that lead to organizational security benefits, including increased security risks awareness, removal of flaws in security defenses, and improved security response. Bartnes et al. (2016) used an inductive case study research approach to understand the challenges for improving information security incident management practices. The authors showed that information security incident response training is given low priority and that different types of personnel, such as business managers and technical personnel, have different perspectives and priorities on information security. Therefore, the authors

called for regular training sessions and systematic evaluations after such sessions. Applying interviews and document analyses, Riebe et al. (2021) researched organizational structures, technology use, and the impact on collaborative practices in and between state CERTs in Germany. Their findings point out e.g., the "cross-platform monitoring and analysis of incident data, use of deduplication techniques and standardized threat exchange formats, a reduction of resource costs through process automation, and transparent reporting and tool structures for information exchange".

Decision Making by Experts under Pressure: Recognition-Primed Decision Making (RPD)

Experienced professionals are likely to use a recognition-based model of decision making in times where they need to make decisions under pressure and uncertainty. This principal finding was encompassed by Klein et al. (1986; Klein, 2008) in a model named 'Recognition-Primed Decision-making' (RPD). RPD is one of the most prominent models of Naturalistic Decision Making and rooted in empirical research of firefighting operations, but also successfully describes decision making for doctors, pilots, chess players, offshore incident managers, and military officers (Klein, 2008; 2009).

According to RPD, professionals working under time pressure and uncertainty possess the ability to recognize a new situation based on a set of indicators and then subsequently to choose an approach which has worked satisfactorily in a similar situation in the past (Klein, 2008). Klein (1993) distinguished between three RPD-models: (1.) a simple match model, (2.) an action strategy model, and (3.) a complex RPD strategy model. In the first and simplest model (simple match), the situation is identified by the decision maker and the most obvious reaction is implemented (Klein, 1993). This model is primarily used when the decision maker has limited time. The second RPD model (developing a course of action) involves the same simple match strategy as in the first model, but the decision maker conducts some conscious evaluation – called mental simulation – of the response to uncover problems prior to implementing it (Klein, 1993). This RPD model is more commonly used in case the decision makers dispose of more time. The third and most advanced RPD model (complex RPD strategy) is used when decision makers, after a deliberate evaluation, find out that the situation does not meet any previous experiences. In this case, the decision maker will try to identify the new situation, including the option that is most suited for that specific situation (Klein, 1993).

Although RPD is often an effective decision making strategy considering the challenging conditions under which decisions must be made, in certain cases it may lead to unsatisfactory decisions. Two specific scenarios can be described:

1. First, personal recognition may hinder judgment. An experienced professional may think that they are dealing with a prototypical situation and thus overlook certain (contradictory) indicators. Especially when working under pressure, the quick situational recognition could impede perceiving conflicting data points. For instance, if an IT application fails during a so-called change window, a CIR consultant might intuitively assume that the outage is caused by the change, thus overlooking the less likely possibility of a deliberate attack (Groenendaal, 2015; Groenendaal & Helsloot, 2016).
2. Second, a lack of detection may occur as a result of the decision maker not having the relevant or correct experience and/or the (learning) environment does not provide accurate feedback. If the environment does not provide timely or accurate feedback, it will be impossible for the decision maker to gain reliable insight into the causality between their actions and consequences thereof (Kahneman & Klein, 2009).

METHODOLOGY

As empirical research methodology, we have used the critical decision method, a retrospective interview strategy developed by Klein et al. (1989) that applies a set of cognitive probes to non-routine or contra-intuitive incidents that required expert judgment or decision making. This methodology has been used extensively to explore decision making under challenging circumstances but, as far as we are concerned, has not been applied to study cyber incident response practices yet.

Critical Decision Method

The critical decision method (CDM) was developed for modelling tasks in naturalistic environments, for instance in firefighting (Klein et al. 1989). It is a retrospective interview strategy in which a series of cognitive tests are

applied to actual, non-routine incidents required expert judgment or decision making (ibid). It is a theory-driven strategy based on the assumption that expertise emerges most clearly during non-routine events and focuses on these as the prime source of information. Once the incident is selected, the interviewer asks for a brief description of the incident. Then, a semi-structured questionnaire is used to explore different aspects of the decision making process. According to Klein et al. (1989), the CDM has the following key characteristics:

- The CDM, like most critical incident techniques, focuses on non-routine cases. Non-routine or difficult incidents usually provide the most fruitful source of data about the capabilities of highly-skilled personnel.
- In an interview using the critical decision method, questions always refer to a specifically recalled incident and decision points.
- Probing in the CDM is not limited to answers that can be objectively validated. Questions sometimes require the decision makers to reflect on their own strategies and decision bases.
- The CDM represents the middle ground between a completely unstructured approach, such as an ongoing verbal protocol, and a completely structured, such as a structured interview.

Interview Procedure

The basic interview procedure of the CDM can be summarized in the following steps (derived from Klein et al. 1989):

1. Select incident: Ask the participant to select an incident that presented a particular challenge,

2. Obtain unstructured incident account: Solicit the participant's description of the incident from the beginning until it is found to be under control,

3. Create a timeline of the incident: Reconstruct the account in the form of a timeline that establishes the sequence and duration of each event reported by the participant,

4. Decision point identification: Ask the participant to indicate specific decisions on the timeline,

5. Decision point probing: To gather more details on the decisions, we used a questionnaire with the following questions:

   a. Cues: What were you seeing, hearing, smelling?

   b. Knowledge: What information did you use in making this decision and how was it obtained?

   c. Analogues: Were you reminded of any previous experience?

   d. Goals: What were your specific goals at this time?

   e. Options: What other courses of action were considered by or available to you?

   f. Basis: How was this option selected/other options rejected? What rule was being followed?

   g. Experience: What specific training or experience was necessary or helpful in making this decision?

   h. Aiding: If the decision was not the best, what training, knowledge or information could have helped?

   i. Time pressure: How much time pressure was involved in the decision making?

   j. Situation assessment: Imagine that you were asked to describe the situation to a relief cyber incident responder at this point, how would you summarize the situation?

   k. Hypotheticals: If a key feature of the situation had been different, what difference would it have made in your decision?

The Interviews were held in Q1 2021 via MS Teams and lasted between 45-60 minutes on average. As all the interviews were conducted digitally via MS Teams, we skipped two steps of the CDM, i.e. the request to the decision maker to draft a timeline and plot the relevant decision points (step 3 and 4).

Participants

In general, finding participants for cyber incident response research is challenging, and recruiting experienced CIR consultants was even more difficult. Worldwide, a shortage of talented cybersecurity experts and particularly experienced CIR consultants appears to exist, while the demand for their expertise is high. Consequently, it is

difficult to find experienced CIR consultants willing to devote time to participate in such studies. Nevertheless, we were able to find six experienced CIR consultants to participate in our research by reaching out to three major CIR service providers in the Netherlands. Table 1 provides a list of the anonymized participants, employers, and their years of experience. CIR consultant 1 is employed by a CIR provider working for a specific sector organization within the Netherlands. The other five CIR consultants that participated in our research are employed by an international CIR service provider.

Table 1: Participants, employers and years of experience in CIR

Participant	Years of Experience in CIR	Gender
CIR consultant 1 (National CIR provider)	5-10 years	M
CIR consultant 2 (International CIR provider 1)	5-10 years	M
CIR consultant 3 (International CIR provider 2)	>10 years	M
CIR consultant 4 (International CIR provider 2)	>10 years	M
CIR consultant 5 (International CIR provider 3)	>10 years	M
CIR consultant 6 (International CIR provider 3)	>10 years	M

EMPIRICAL FINDINGS

Our analysis reveals that CIR consultants recognize situations based on past experiences but tend to wait to act until they have gathered and evaluated all available facts. The respondents indicated that they often have a main hypothesis but want to collect and analyze all the available evidence before making any decisions. For example, CIR consultant 5 elaborated:

> "The entry point of most attackers is usually phishing, a compromised third-party or an exploited vulnerability. After a quick assessment of the environment, you know what is going on a high-level. But you want to be sure. I don't want to jump to conclusions."

As CIR consultant 1 stated: "My mindset is: maybe I've missed something. I need to dig deeper." Or, as put forward by CIR consultant 2:

> "You should always have the feeling that you have not detected everything. The goal is to strive to find every possible attack vector before you act. That is why a combination of real time threat intel, perseverance, and a good team is conditional for effective cyber incident response. You need to find all compromised hosts."

Similarly, CIR Consultant 3 noted: "But of course the analysis phase must stop somewhere. I can never be a 100% sure that I have identified everything. But you want to minimize the chance that you haven't found something before you act." Finally, CIR consultant 6 pointed out something similar: "You always want to do as many sweeps as possible before you start acting."

All respondents mentioned that one of the most difficult and recurring decisions during a major network breach, is deciding when to move from investigation to eradication (i.e. removing an attacker from the network and implementing security improvements to prevent the attacker from quickly regaining access to the environment). In the words of CIR Consultant 2: "When to remove the threat? That is the one-million-dollar question." According to CIR Consultant 4, there are basically three ways of eradication. The first and preferred way is incident containment. "This is a strategical surgical strike to the attacker's ability to access specific resources in the environment. The goal is not to disrupt but to surgically limit the organization's exposure." The second way is described as a game of whack-a-mole. "It is what we describe as the unplanned, iterate, and systematic process of blocking the attacker in small little steps as the investigation discovers attacker activity." The third way is disruption. "The aim with disruption is to significantly impede the attacker's ability to achieve its goals. A keyword in this case seems 'significant'." All respondents agreed that eradication should be performed in a concise

and coordinated manner, a 'single blow'. However, this does not always succeed, which means that whack-a-mole or disruption strategies must be implemented. As stated by CIR Consultant 5:

> "I was hired by a customer in South Korea. A large gaming company was breached to steal signing certificates. The attacker used a self-propagated backdoor, which basically infected the binaries. You can see this as a virus component with a backdoor in it. We were chasing the attacker for months. It was playing whack-a-mole. We killed ten infected systems, and 15 more showed up the next day. For us, the aim was to defeat the attackers. At one day, we had a meeting with the Chief Operating Officer (COO), the executive response for the operations of the company. In hindsight, the COO made a difficult but wise decision. The COO said: Let's stop here. We will stop and rebuild the company's IT infrastructure from scratch."

All respondents stated that eradication should occur in the striking zone. CIR Consultant 3 indicated that: "You can be too early, too late, or just in time. If you eradicate in time, this is what we call the striking zone." According to CIR consultant 4, conducting eradication in the striking zone requires a deep understanding of the extent of the compromise, knowledge of the attacker's tactics, and the ability to reliably detect malware and tools leveraged by an attacker. There are several risks involved with starting the eradication too early or too late. According to CIR consultant 2, if eradication starts too late there is a risk that the attacker can steal valuable information, which could have been prevented, if eradication had started earlier. Or it could result in the attacker installing ransomware and encrypting the network, causing prolonged network outage. Furthermore, the attacker may become inactive, e.g. stops activities, causing the investigation to lose track. Remedying too early might attract the attacker's attention to the investigation and may cause them to change their tactics, techniques, and procedures. This could result in the attacker's actions becoming invisible or enraged, causing even more systems being attacked or disrupted. For us, in summary, the key question is how experienced CIR consultants decide about the time when they need to be in the striking zone and about the procedure of the eradication.

The analysis revealed that all respondents apply the simple-match RPD model when making decisions about when to move from investigation to eradication. As a general rule of thumb, the CIR consultants use a 'watch and learn strategy' which implies investigating as much as possible and learning from the attacker's behavior. Only if the situation is recognized to be threatening (e.g. the attacker is wiping their traces or installing specific malware), is eradication considered. In this regard, CIR Consultant 6 mentioned that:

> "You have to make a decision what to do when you get to a client. You have only very little information at your disposal. There is a certain degree of time pressure. On the one hand, you need to learn the environment and the behavior of the attacker. On the other hand, the client wants you to protect its data. My recommended strategy by default is to take time to understand what the attacker is doing. You do not want to remediate too early. If the attacker knows s/he is being caught, then s/he can hide himself/herself or start disrupting the network. I want to prevent that".

CIR Consultant 4 had a similar opinion:

> "My initial strategy and advice to clients would always be to observe and buy as much time as possible to learn about the attackers and their modus operandi. By doing this, you have more certainty about the size of the breach and a better understanding of how the attacker works. If you remove an attacker too early from the environment, you might miss certain entry points which allows the attacker to come back without you knowing. By reacting too early, you are essentially teaching the attacker what we can and can not see as we play what I call whack-a-mole."

In rare occasions, however, the watch and learn strategy turned out to be wrong in the aftermath. CIR consultant 5 mentioned that:

> "Three years ago, I supported a client in Asia. It was a telco environment. The telco was under attack. Attackers had been in the environment for multiple years. When we discovered that, the customer's first reaction was 'please remove the system from the network', this led to a fierce discussion in which we advised the customer not to remove it yet. We wanted more time to search for more indicators of compromise. The client agreed with our advice. When I woke up next morning, we discovered that the attacker downloaded 500 gigabytes of data during the night via a web shell. This incident led to a

> difficult conversation with the client. In hindsight, it would have been better to remove that web shell. But still, by removing the web shell, you drive the attacker into your blind spot. You are basically teaching the attacker what you can see."

Although the most common used practice, in the majority of incidents, is observing and learning, there are some exceptions which could occur suddenly and require immediate eradication. The respondents stated that there are several indicators that could signal an 'a-typical situation', in which immediate eradication seems the best option. As addressed by CIR Consultant 5:

> "There are several cases in which you need to start eradicating immediately. For instance, if you suspect that an attacker is using ransomware and is about to decrypt the systems, quick eradication is recommended. Furthermore, if you find out that the attacker has access to 'nuclear launch codes', or whatever the equivalent is for that specific business, you need to start eradicating. Other reasons to eradicate quickly are when you know that you have caught the attacker early on in the intrusion lifecycle or when you notice that the attacker is moving out of your radar."

When asked how the decision is made to switch from observing and learning to eradicating, most respondents cited following their intuition. CIR Consultant 6 mentioned in this regard that:

> "It is an intuitive decision. It also depends per situation. For me, clear triggers that require me to reassess the situation are facts that indicate large data exfiltration, a dump of the active directory or indications that the attacker is changing his tactics. Then you have to act, even if you don't have full certainty about what is going on."

Another example that shows that CIR consultants apply RPD relates to paying the ransom following a ransomware attack. All respondents mention that during a ransomware attack, the advice whether or not clients should pay the ransom as requested by the attacker is often a challenging situation. As stated by CIR Consultant 6:

> "We advised a large media company. The company was hit by ransomware. The impact was huge: more than 1000 servers were encrypted and about 6000 employees were unable to work. The primary processes of the company were completely disrupted. The client did not know what to do. They completely relied on our expertise. They look at us. If we say, you should pay, they will pay. If we say, don't pay, they often do not do it. Of course, in the end, it is the client that makes the final decision. But my experience is that they often do what we advise."

All respondents indicate that as a general rule of thumb, the advice to clients is to not pay the ransom and to find other ways to retrieve or restore the data. CIR Consultant 1:

> "In 99% of the cases this would be my initial advice based on my experience. Hence, when hired to support during a ransomware attack, my initial advice would be not to pay the ransom and investigate whether the data could be retrieved in another way."

Some of the respondent's stated that they advise clients to pay a ransom in some particular instances. This is the case when the initial recognition of the situation is reassessed after all expectations about the situation are violated. For instance, when it appears to be impossible to restore the back-ups or find workarounds that enable a quick recovery of the most important business processes. Another instance might bewhen the business impact is so significant that the survival of the organization is at stake. When the initial situation is reassessed and recognized as 'hopeless' and threatening to the survival of the organization, then the obvious advice to the client would be to pay the ransom. CIR Consultant 3:

> "If you don't have any other option and the business is totally disrupted, then I would advise the client to pay the ransom. This means that you have assessed all alternatives."

Paying the ransom is recognized by CIR Consultant 1, 2 and 5 as an undesirable but effective way to retrieve data and quickly bring the organization back in business. But, as explained by CIR Consultant 6, there can always be exceptions. CIR Consultant 6:

> "We were hired by a logistics company responsible for food distribution to others supermarkets. Based

on our initial investigation, we concluded that the ransomware attack was advanced and it would take weeks or even months to get everything back in business. Based on the business context, we advised the client to pay the ransom. We received the encryption key from the attacker, but it was not working well. Consequently, the client paid a lot of money but much of the data was still unusable. This was a worst-case scenario that we rarely encounter. In 99% of the cases, you will get your data back once you pay the ransom."

ANALYSIS AND DISCUSSION

In this preliminary research, we investigated (1) to what extent do experienced CIR consultants apply RPD during their work and (2) what are the implications for cyber crisis management, training, and decision-aiding. In order to answer both questions, we conducted six in-depths interviews with experienced CIR consultants from different countries. The interviews revealed that the respondents use RPD in the sense that they look for clues that describe the situation in terms of the type of the cyber breach encountered and then apply a course of action that has worked effectively in the past. This course of action seems to be characterized by collecting and evaluating more data in a way that depends on the exact cyber breach before initiating further action. In the majority of cases, this course of action results in appropriate outcomes, as may be expected from an expert. However, as discussed in the results section, we have also seen exceptional situations in which this course of action led to unnecessary data theft and damage.

The finding that CIR consultants would use RPD during their work met our expectations, as we assumed that CIR consultants' work context has much in common with other operational domains such as military, firefighting and aviation. However, we were surprised by the fact that the common course of action is characterized by watch and learn strategies and buying time. This finding differs from the aforementioned operational domains where recognition is usually followed immediately by prompt action (e.g. Groenendaal & Helsloot, 2016).

The finding above has an important direct implication, i.e. that CIR consultants that confront a cyber breach will use the 'seek more information' approach as the standard course of action because it is mostly correct. In the rare situations that this is not the optimal course of action *somebody other* than the CIR consultant alerted for the cyber breach should decide that immediate action is necessary.

Implications for Cyber Crisis Management

During a cyber crisis – i.e. an unexpected event caused by a cyber threat or incident that seriously threatens or impacts organizational assets and requires decision-making under time pressure and uncertainty – the cyber crisis management team needs to provide strategic direction to the cyber incident response operation. The findings of our preliminary research suggest that crisis management teams should decide to what extent and in what ways they want to mitigate the risk of responding belatedly to cyber events, which could potentially lead to unnecessary data theft and sustained business disruption. First, this implies that the cyber crisis management team must define the objectives of the crisis response. If the objective is to get back in business as quickly as possible, then watch and learn strategies are not favorable and CIR consultants should be directed to initiate eradication. On the other way, if attribution of the attack is deemed important, then watch and learn strategies would be more suitable. Second, cyber crisis management teams should set the boundaries for external CIR consultants. These boundaries include amongst others what additional data loss or damage is tolerated (if any) and the budget that the organization is willing to spend on external CIR services.

Another implication of our preliminary research is that crisis management teams should consider whether additional forensic investigations outweigh the expected benefits throughout the response process. Our findings suggest that CIR consultants find it difficult to stop the investigation themselves when not all facts have been gathered (e.g. if the likely entry-point of the attacker has been discovered how much effort should be devoted to exclude other potential entry-points?) or when the evaluation of facts does not provide a clear picture (e.g. based on the investigation it cannot be concluded what data is exfiltrated exactly).

Implications for Training and Decision Making

Based on our preliminary research, we would recommend CIR practitioners to take notice of the NDM framework and particularly RPD. When training CIR professionals, RPD should be explained, including the exceptions in

which this default strategy does not work well. Novice CIR professionals should be taught how to recognize these exceptions (e.g. what cues to look for) and what alternate strategies could work in these exceptional situations. Finally, several biases related to 'information hunger' or 'information addiction' (e.g. Helsloot & Groenendaal, 2011) should be discussed as well. Insights from NDM may be used to improve decision making of CIR professionals. NDM insights can be used to develop decision aids or tools to improve decision making. For instance, Groenendaal (2015) developed a model of incident command based on NDM insights that could be applied to cyber incident response. This model could help leaders of CIR teams to identify vulnerabilities in the decision making of team members and provide suggestions to reduce the likelihood of suboptimal decisions.

Again, according to the RPD model, it may never be expected from an experienced CIR consultant who is alerted for a cyber breach and is working on it, to be able to change their course of action. Someone else should decide upon this.

Limitations

Our research suffers from several limitations and we therefore stress that it should be considered as a preliminary study. First and foremost, it should be noted that our preliminary research is based upon a small data set of only six experienced CIR consultants. Due to the small data set and non-representative sample, the findings of our research have to be validated by more research before they can be generalized. The second limitation is that we relied on respondents' perception of their decision making – which could be flawed, rather than a participatory observation of their actual decision making during incident response assignments. Therefore, we recommend for researchers to combine various research methods when doing research on CIR decision making like case study analysis, interviews and direct observation.

In addition, we recommend researchers conduct more research to the applicability of other NDM models within a CIR context. In this research we focused on RPD, but there are other NDM models that could also be applied to gain a better understanding of CIR decision-making, such as the image theory, situation awareness, or explanation-based decision making. Furthermore, more research is necessary to understand how the team context influences decision making. For instance, we assume that team size, team roles, and experience of team members working with each other will influence the decision making process and even team performance.

CONCLUSION

We conclude that in order to enhance cyber resilience more insight is necessary in CIR decision-making. Our research suggests that CIR consultants can not be expected to act directly unless, in the rare circumstance, this should be required by the situation. For such situations another decision making mechanism should be established. We stress that more research with a larger sample size is necessary to validate our findings.

ACKNOWLEDGMENTS

This paper is a revised and extended version of Groenendaal et al. (2020). We thank all authors, program and local committee members, and volunteers for their hard work and contributions to the ISCRAM conference.

REFERENCES

Ahmad, A., Hadjkiss, J., & Ruighaver, A.B. (2012). Incident Response Teams - Challenges in Supporting the Organizational Security Function. Computers & Security. 31(5), (pp. 643–652).

Ahmad, A., Maynard, S.B., Desouza, K.C., Kotsias, J., Whitty, M., & Baskerville, R.L., (2021). How can Organizations Develop Situation Awareness for Incident Response? A Case Study of Management Practice. Computers & Security. Vol 101. (pp. 1-15).

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. Journal of the Association for Information Science and Technology, 71(8), 939-953.

Bartnes, M., Moe, N. B., & Heegaard, P. E. (2016). The future of information security incident management training: A case study of electrical power companies. Computers & Security, 61, 32-45.

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered Information Security: Managing a Strategic

Balance between Prevention and Response. Information & Management, 51(1), 138-151.

Beach, L. R. (1990). Image theory: Decision making in personal and organizational contexts. New York: John Wiley & Sons.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2002). Assessing the value of detective control in IT security. AMCIS 2002 Proceedings, 263.

Cichonski, P., Millar, T., Scarfone, K. (2012). Computer Security Incident Handling Guide. National Institute of Standards and Technology

Conolly, T., & Koput, K. (1997). Naturalistic decision making and the new organizational context u: Shapira, Z.(Ed.), Organizational Decision Making. Cambridge University Press.

Freiling, F. C., & Schwittay, B. (2007). A common process model for incident response and computer forensics. IMF 2007: IT-Incident Management & IT-Forensics.

Groenendaal, J. (2015). Frontline Command: Reflections on practice and research. Den Haag: Eleven International Publishing.

Groenendaal, J., & Helsloot, I. (2016). The application of Naturalistic Decision Making (NDM) and other research: lessons for frontline commanders. Journal of Management & Organization, 22(2), 173-185.

Groenendaal, J. Barjas, S. & Helsloot, I. (2020). Cyber incident response decision making: What can be learned from experienced Cyber Incident Response Consultants? A preliminary investigation. The Hague University of Applied Sciences & Crisislab, The Hague and Renswoude.

Groenendaal, J., & Helsloot, I. (2021). Cyber resilience during the COVID-19 pandemic crisis: A case study. Journal of Contingencies and Crisis Management.

Gutzwiller, R. S., Ferguson-Walter, K. J., & Fugate, S. J. (2019, November). Are cyber attackers thinking fast and slow? Exploratory analysis reveals evidence of decision-making biases in red teamers. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 63, No. 1, pp. 427-431). Sage CA: Los Angeles, CA: SAGE Publications.

Helsloot, I., & Groenendaal, J. (2011). Naturalistic decision making in forensic science: Toward a better understanding of decision making by forensic team leaders. Journal of forensic sciences, 56(4), 890-897.

Klein, G. A. (1993). A recognition-primed decision (RPD) model of rapid decision making. Decision making in action: Models and methods, 5(4), 138-147.

Klein, G. (1998). Sources of power: How people make decisions. Cambridge, MA: MIT Press.

Klein, G. (2008). Naturalistic decision making. Human Factors: The Journal of the Human Factors and Ergonomics Society, 50(3), 456-460.

Klein, G. (2009). Streetlights and shadows: Searching for the keys to adaptive decision making. London, England: The MIT Press.

Klein, G., Calderwood, R., & Clinton-Cirocco, A. (1986). Rapid decision making on the fireground. In Proceedings of the Human Factors and Ergonomics Society 30th Annual Meeting (Vol. 1, pp. 576–580). Norwood, NJ: Ablex.

Klein, G. A., Calderwood, R., & Macgregor, D. (1989). Critical decision method for eliciting knowledge. IEEE Transactions on systems, man, and cybernetics, 19(3), 462-472.

Lipshitz, R., Klein, G., Orasanu, J., & Salas, E. (2001). Taking stock of naturalistic decision making. Journal of behavioral decision making, 14(5), 331-352.

Morgeson, F. P., Aiman-Smith, L.D., & Campion, M.A. (1997). Implementing work teams: recommendations from organisational behaviour and development theories. In M.M Beyerlein, D.A. Johnson & S.T. Beyerlein (Eds). Advances in interdisciplinary studies of work teams (Vol 4, pp. 1-44). Amsterdam: Elsevier Science & Technology Books

Pennington, N., & Hastie, R. (1988). Explanation-based decision making: effects of memory structure on judgment. Journal of Experimental Psychology: Learning, Memory, and Cognition, 14(3), 521.

Rajivan, P., & Cooke, N. J. (2018). Information-pooling bias in collaborative security incident correlation analysis. Human factors, 60(5), 626-639.

Riebe, T., Kaufhold, M.-A. & Reuter. C. (2021). The Impact of Organizational Structure and Technology Use on Collaborative Practices in Computer Emergency Response Teams: An Empirical Study. Proceedings of the ACM: Human Computer Interaction (PACM): Computer-Supported Cooperative Work and Social Computing 5, Nr. CSCW2 (2021). https://doi.org/10.1145/3479865.

Simon, H. A. (1955). A behavioral model of rational choice. The Quarterly Journal of Economics, 69(1), 99-118.

Srinivas, J., Das, A, K., Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations, Future Generation Computer Systems, Volume 92, (pp. 178-188).

van der Kleij, R., Schraagen, J. M., Cadet, B., & Young, H. (2022). Developing decision support for cybersecurity threat and incident managers. Computers & Security, 113, 102535.

Zager, R., & Zager, J. (2017). OODA loops in cyberspace: A new cyber-defense model. Journal Article| October, 20(11), 33pm.

Zimmerman, C. (2014). Cybersecurity Operations Center. The MITRE Corporation.

Zsambok, CE. & Klein, G (1997) Naturalistic Decision Making. Mahwah, New Jersey: Lawrence Erlbaum Associates.