Cyber incident response decision making: What can be learned from experienced Cyber Incident Response Consultants?

A preliminary investigation

Authors:
Dr Jelle Groenendaal
Saman Barjas MSc
Prof. Dr Ira Helsloot
(Radboud Universiteit Nijmegen)

let's change
YOU. US. THE WORLD.

THE HAGUE
UNIVERSITY OF
APPLIED SCIENCES

The Hague University of Applied Sciences
Johanna Westerdijkplein 75
2521 EN The Hague
www.thehagueuniversity.com

Authors:
Dr Jelle Groenendaal
Saman Barjas MSc
Prof. Dr Ira Helsloot (Radboud University Nijmegen)

Photos/illustrations: Shutterstock.com
Design: Education, Knowledge & Communication

Management Summary

In case of a major cyber incident, organizations usually rely on external providers of Cyber Incident Response (CIR) services. CIR consultants operate in a dynamic and constantly changing environment in which they must actively engage in information management and problem solving while adapting to complex circumstances. In this challenging environment CIR consultants need to make critical decisions about what to advise clients that are impacted by a major cyber incident.

Despite its relevance, CIR decision making is an understudied topic. The objective of this preliminary investigation is therefore to understand what decision-making strategies experienced CIR consultants use during challenging incidents and to offer suggestions for training and decision-aiding.

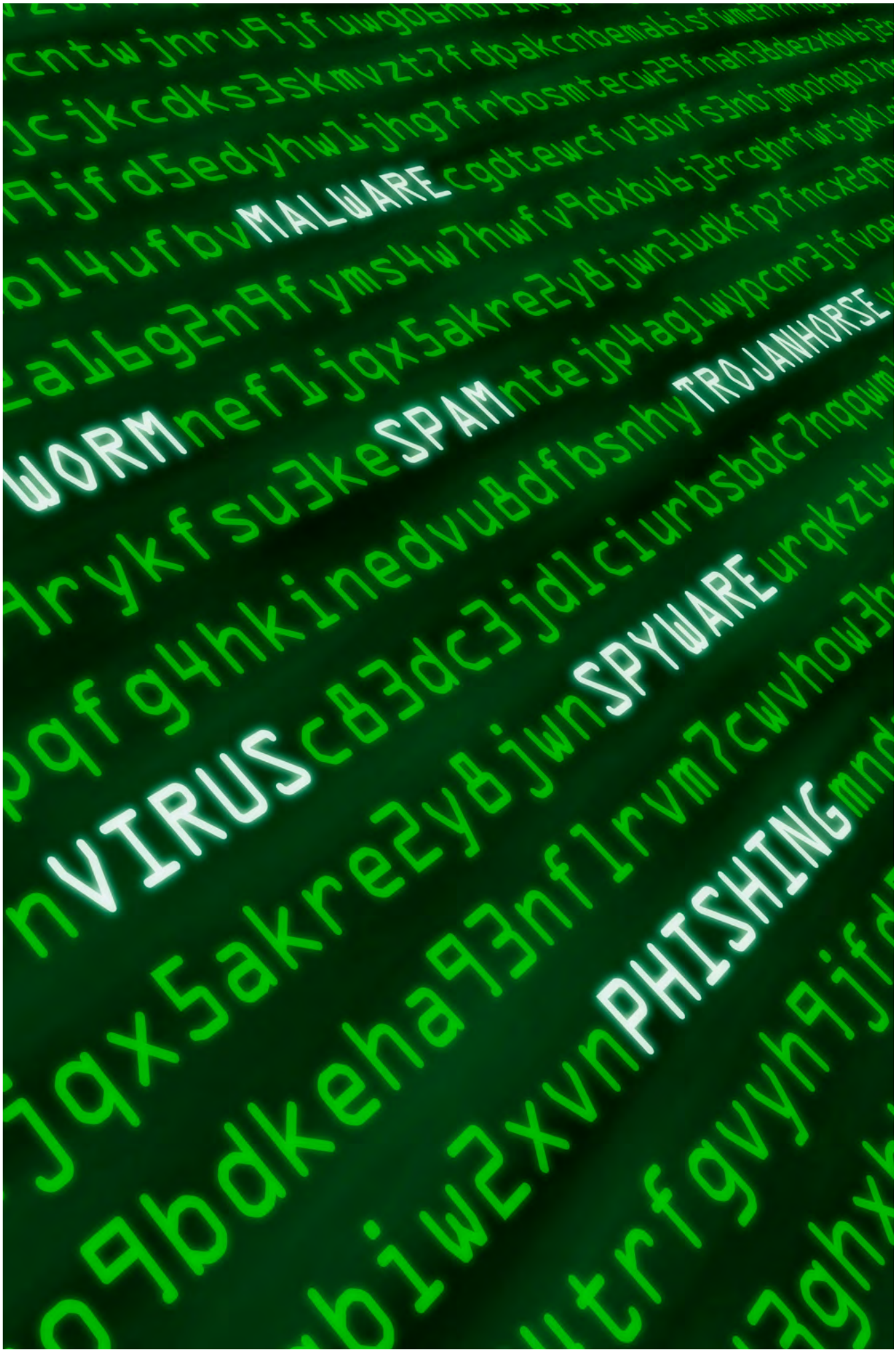
A general understanding of operational decision making under pressure, uncertainty, and high stakes was established by reviewing the body of knowledge known as Naturalistic Decision Making (NDM). The general conclusion of NDM research is that experts usually make adequate decisions based on (fast) recognition of the situation and applying the most obvious (default) response pattern that has worked in similar situations in the past. In exceptional situations, however, this way of recognition-primed decision-making results in suboptimal decisions as experts are likely to miss conflicting cues once the situation is quickly recognized under pressure.

Understanding the default response pattern and the rare occasions in which this response pattern could be ineffective is therefore key for improving and aiding cyber incident response decision making. Therefore, we interviewed six experienced CIR consultants and used the critical decision method (CDM) to learn how they made decisions under challenging conditions.

The **main conclusion** is that the default response pattern for CIR consultants during cyber breaches is to reduce uncertainty as much as possible by gathering and investigating data and thus delay decision making about eradication until the investigation is completed. According to the respondents, this strategy usually works well and provides the most assurance that the threat actor can be completely removed from the network. However, the majority of respondents could recall at least one case in which this strategy (in hindsight) resulted in unnecessary theft of data or damage.

Interestingly, this finding is strikingly different from other operational decision-making domains such as the military, police and fire service in which there is a general tendency to act rapidly instead of searching for more information.

The **main advice** is that training and decision aiding of (novice) cyber incident responders should be aimed at the following: (a) make cyber incident responders aware of how recognition-primed decision making works; (b) discuss the default response strategy that typically works well in several scenarios; (c) explain the exception and how the exception can be recognized; (d) provide alternative response strategies that work better in exceptional situations.


MALWARE
WORM
SPAM
TROJANHORSE
VIRUS
SPYWARE
PHISHING

INHOUDSOPGAVE

1 Introduction

1.1 Research Background

Research and practice increasingly recognize that cyber incidents cannot be completely prevented. The cyber research and practice domain does therefore follow the Normal Accident Theory paradigm (Perrow, 1984) which states that incidents are inevitable because systems are getting increasingly complex, highly interactive, and tightly coupled. Therefore, organizations must be prepared to deal with potential breaches. This recognition is captured in the concept of *cyber resilience*. Cyber resilience starts with the acceptance of cyber compromise as a likely event and the organization suffering as a result (Kott & Linkov, 2021). Cyber resilience then focusses on the ability to make sense of wat what happens after an adverse cyber event and on the preparedness to handle both known and unknown cyber threats (Kott & Linkov, 2021). Contrary to cybersecurity that focusses on prevention of an attack, cyber resilience thus puts the focus on the organization's ability to absorb, recover and adapt, and not just resist (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 this response ability is **cyber incident response (CIR)**. CIR is the organizational capability aimed at detecting the occurrence of an incident, containing the impact of the incident as much as possible and eradicating the threat from the organization (Ahmad et al. 2021). Organizations implement CIR capabilities in diverse configurations. Small to medium sized organizations usually do not have a dedicated CIR capability. CIR in these organizations is organized ad-hoc and could be conducted by the IT manager, a small group drawn from the IT unit, or an outsourced IT service provider (see for instance Ebbers et al. 2020). Large organizations usually have a dedicated CIR capability consisting of a Security Operations Center (SOC), which can be insourced or outsourced, for continuous monitoring, investigation and response to cyber threats and incidents. In some of these organizations the SOC is complemented with a Computer or Cyber Incident Response Team (CIRT), which adds additional technical expertise for threat analysis and incident response (Ahmad et al. 2021).

However, in case of a major cyber incident existing CIR capabilities might not be sufficient. Organizations typically lack the resources and expertise to deal with advanced cyber incidents alone. Therefore, they rely on external commercial providers of CIR services to come to their aid. External CIR service providers offer services to organizations that need immediate assistance with the analysis (e.g. determine the causes), containment (e.g. prevent further damage), eradication (e.g. remove the threat from the environment), and recovery (e.g. recover lost information and reduce future vulnerabilities) of suspected or confirmed cyber incidents. Organizations can hire CIR service providers proactively in anticipation of possible attacks (e.g. through a retainer) or reach out upon learning of a (potential) cyber incident.

CIR service providers employ highly skilled and experienced CIR consultants focusing on forensic analysis, reverse malware engineering, threat investigation, and incident coordination amongst others. As these CIR consultants are involved in incident response activities on a daily basis and have gained experience in many different organizations, they are among the most experienced professionals in their field. As a consequence, much can be learned from the way these experienced professionals make decisions under challenging conditions. This research is a preliminary attempt to gain insight into the way experienced external CIR consultants make decisions and to draw lessons for training and decision-aiding.

1.2 Problem Analysis

CIR consultants operate in a dynamic and constantly changing environment in which they must actively engage in information management and problem solving while adapting to complex circumstances (Steinke et al. 2015). In this challenging environment, external CIR consultants need to make critical decisions about what to advise clients that are impact by a major cyber incident. For instance, they advise clients whether or not a ransom should be paid in case of a ransomware attack. Or they determine when an attacker must be removed from the IT network and advise clients accordingly. The consequences of these decisions can be high and typically the decision-making process is characterized by time pressure and uncertainty. Consequently, effective decision making is extremely difficult but at the same time, key to keep the impact of the cyber incident for the client as limited as possible.

> In case of a cyber incident such as a ransomware attack, a decision made by an external CIR consultant can mean the difference between becoming fully operational again within a few days or having to build a new IT network resulting in a significant business disruption. Or similarly in case of an advanced persistent threat, the external CIR consultant need to advise the client when the intruder should be removed from the network. If you wait too long with removing the threat actor from the network, information may be unnecessarily stolen. If you intervene too quickly, you may have insufficient insight into the intruder's way of working and thereby giving the intruder the opportunity to hide again and become invisible.

Despite its relevance, CIR decision making is an understudied topic. Previous research primarily focused on organization and management aspects of cyber incident response (see Chapter 2 for some examples). Much less scholarly attention has been devoted to the way cyber incident responders, individually and in team settings, assess information and make decisions during their incident response tasks. However, CIR decision making deserves more research attention as it is generally acknowledged in the academic literature that effective cyber incident response requires incident responders and teams to make appropriate 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 has parallels with operational command in other domains. Much research has already considered the way in which experts make operational decisions under challenging conditions. This research concerns what is known as naturalistic decision making, or NDM. According to Zsambok & Klein (1997: 5), NDM research studies how experienced people, working as individuals or groups in dynamic, uncertain, and often fast-paced environments, identify and assess their situation, make decisions and take actions whose consequences are meaningful to them and to the larger organization in which they operate. NDM research covers decision making studies in various operational domains such as the military, fire service, police, emergency health care and aviation. However, the question is to what extent insights from NDM research also apply to CIR decision making. Therefore, this research is aimed at learning how experienced CIR consultants make decisions during their incident response work and what can be learned from the way they make decisions for training and decision-aiding.

1.3 Research Objectives

The objectives of this preliminary investigation are to understand what decision-making strategies experienced CIR consultants use during challenging incidents and to offer suggestions for training and decision-aiding.

1.4 Research Question

This preliminary investigation is aimed at gaining a better understanding of CIR decision making which forms the basis for their advice and the course of action they initiate. We are particularly interested in the way experienced external CIR consultants make decisions during *challenging incidents* as these occasions reveal the expertise required to be an effective incident responder (c.f. Klein et al. 1986). By studying in detail the general knowledge, specific information and reasoning processes of experienced CIR consultants, we want to gather insights that can be used for training and decision-aiding purposes.

Therefore, the main research question of this preliminary investigation is as follows:

What decision-making strategies do experienced CIR consultants use during challenging incidents and what are the implications for training and decision-aiding?

1.5 Practical Relevance

Novice incident responders and incident responders with little experience (i.e. some larger organizations have dedicated incident response professionals but rarely encounter major cyber breaches) are likely to benefit from the decision-making strategies used by external CIR consultants (who are usually much more experienced due to the nature of their work). Therefore in this research we attempt to elicit external CIR consultants' thinking and cognitive work informing their decisions. The models and strategies used by experienced CIR consultants can be used in the development of education and training activities for novel incident responders and decision-aiding (e.g. checklists, information management system, decision protocols).

1.6 Reading Guide

This research report is structured as follows. Chapter 2 (Theory) of this report provides an initial view of the academic literature on cyber incident response and decision making. Chapter 3 (Research Methodology) describes the research methodology including the interview process and participants. Chapter 4 (Results) reports on the results of our investigation. Chapter 5 (Discussion and Conclusions) puts the results of our research in a broader context and answers the research questions. Chapter 6 (Recommendations) provides initial recommendations for research and practice.

2 Theory

In this chapter, we describe the cyber incident response process, discuss previous research on cyber incident response decision making and explain how experienced professionals under time pressure make decisions.

2.1 Cyber incident response process

This cyber incident response process is intended to contain the threat, eradicate changes in the environment made by the adversary, remove the adversary from the environment, and restore normal operations. The cyber incident response process mainly consists of three main activities (Freiling & Schwittay, 2007):

Initial response: The main objectives in this step include assembling the response team, intake with the client, reviewing network-based and other readily available data, determining the type of incident, and assessing the potential impact. The goal is to gather enough initial information to allow the team to determine the appropriate response.

Investigation: The main objectives in this step are to determine the facts that describe what happened, how it happened, and in some cases, who was responsible.

Remediation: The main objectives in this step are to deploy remediation plans. The remediation plan takes into account factors from all aspects of the situation, including legal, business, political, and technical.

In practice there are multiple models on which to draw 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).

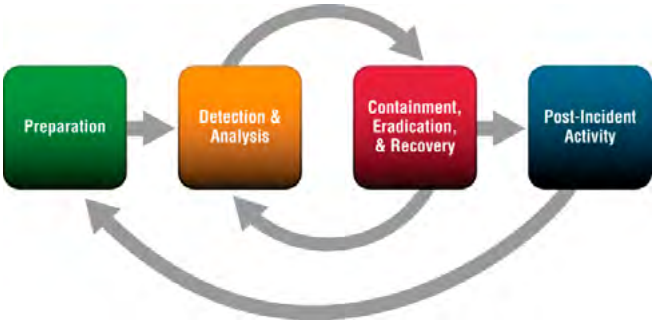


Figure 1 - The NIST incident response life cycle

Another model that is being used is the OODA Loop. The OODA Loop is originally be developed by the military and stands for four tasks: observe, orient, decide, and act.

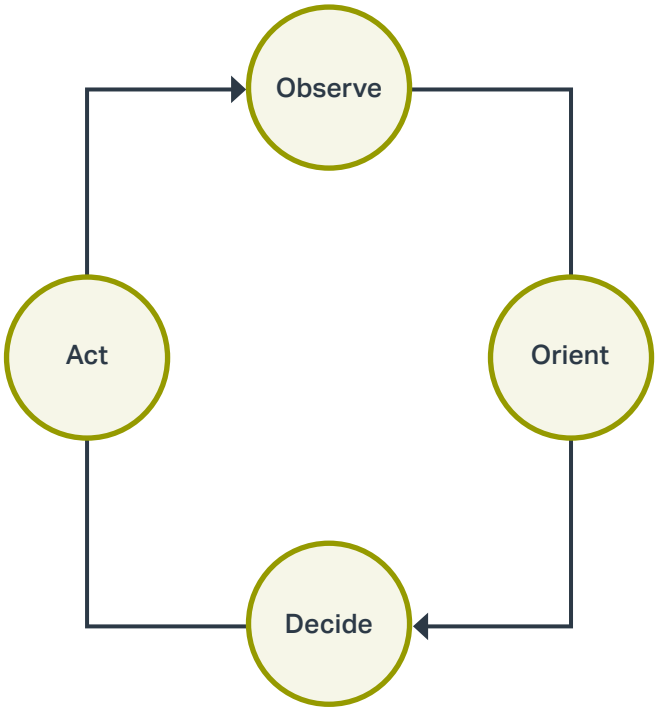


Figure 2 - OODA Loop

Whether organizations are preparing for battle or preparing to respond to a system breach, they are constantly observing the internal and external environments. First, organizations have to put these observations into some sort of context (who, what, where, when, why, how), to orient them as to how the observations might affect us and gather options to respond. Organizations then make decisions as to how to address these events based on the best knowledge. And, if necessary, they then take action (Zager, & Zager, 2017).

The cyber incident response process usually performed by a team of cyber incident responders with different tasks:

- Incident response coordinator
  - The incident response coordinator is responsible for management of the team prior to, during, and after an incident.
- IT security analyst(s)
  - Security analysts perform different duties, ranging from threat hunting, intelligence gathering, and reverse malware engineering. Usually multiple IT security analysts are part of the response team.
- Forensic investigator(s)
  - Forensic investigators are responsible for the forensic analysis, which means securing facts and establishing a time line that eventually can be used in court.

2.2 Previous research on CIR

As stated before, cyber incident response is an understudied research domain. Previous research 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 cyber-threat 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. Ahmad et al. (2012) conducted an exploratory in-depth case study to examine shortcomings in the practice of incident response. The case study revealed the practice of incident response, in accordance with detailed best-practice guidelines, tended to adopt a narrow technical focus aimed at maintaining business continuity whilst neglecting strategic security concerns. The study also discovered that the limited post incident review process focused on 'high-impact' incidents rather than 'high-learning' incidents and 'near misses'. In another study, Ahmad et al. (2020) draws on organizational learning theory to develop a conceptual framework that explains how information security management and incident response functions can create learning opportunities that lead to organizational security benefits including increased awareness of security risks, removal of flaws in security defences and enhanced 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 training for responding to information security incidents is given low priority and that different types of personnel, such as business managers and technical personnel, have different perspectives and priorities in regard to information security. Therefore, the authors called for regular training sessions and systematic evaluations after such sessions.

2.3 Decision making by experts under pressure: Recognition-primed decision making (RPD)

Experienced professionals are likely to use a recognition-primed model of decision making when they have 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 has also successfully described decision making among doctors, pilots, chess players, offshore incident managers, military officers, and other professionals (Klein, 2008; 2009).

According to RPD, professionals working under time pressure and uncertainty possess the ability, on the basis of a number of indicators, to recognise a new situation and subsequently to choose an approach which, in a similar situation in the past, has worked satisfactorily (Klein, 2008).

Table 1: Differences between recognition-primed decision making and classical choice model of decision making (Klein, 1998; 2008)

Recognition-primed decision making (Context: time pressure, high stakes, uncertainty)	Rational choice model of decision making (Context: no time pressure, more information available)
First option is usually workable	Random generation and selective retention
Serial generation of options	Concurrent evaluation of options
Satisficing	Optimising
Evaluation through mental simulation	Evaluation through decision analysis or statistics
Focus on elaborating and improving options	Focus on choosing between options
Focus on situation assessment	Focus on decision events
Decision maker primed to act	Decision maker primed to analyse

Klein (1993) distinguished between three RPD-models: a simple match model, developing a course of action model, and a complex RPD strategy. In the first and most simple model (simple match), the situation is recognized by the decision maker and the obvious reaction is implemented (Klein, 1993). This model is mainly used when the decision maker has little time available. The second RPD model (developing a course of action) covers the same simple match strategy as in the first model, but now the decision maker performs some conscious evaluation – called mental simulation – of the reaction to uncover problems prior to carrying it out (Klein, 1993). This RPD model is more often used when the decision makers have more time at their disposal. The third and most advanced RPD model (complex RPD strategy) is used when decision makers, after conscious evaluation, judge the option inadequate and reject it in favour of the next most typical reaction (Klein, 1993). According to this model, decision makers perform the simple situation match strategy until too many expectations are violated and the situation needs to be reassessed (Klein, 1993). Then the decision maker will try to recognize the new situation including the option that is obvious for that specific situation (ibid).

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

- First, recognition may hinder judgment. An experienced professional can think that they are dealing with a prototypical situation and overlook certain (contradictory) indicators. Especially when working under pressure, the fast recognition of the situation could impede perceiving conflicting data points. For instance, when an IT application goes down during a so-called change window, a CIR consultant might intuitively assume that the outage is caused by the change and hence could overlook the less likely possibility of a deliberate attack (Groenendaal, 2015; Groenendaal & Helsloot, 2016).
- Second, there may be a lack of recognition because the decision maker does not have the relevant or correct experience and/or the (learning) environment does not provide reliable 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 his or her actions and their consequences (Kahneman & Klein, 2009).

3 Research methodology

As primary 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 research decision making under challenging circumstances but, as far as we are concerned, has not been applied to study cyber incident response practices.

3.1 Critical decision method (CDM)

A critical decision method (CDM) is developed for modelling tasks in naturalistic environments (Klein et al. 1989). It is a retrospective interview strategy that applies a set of cognitive probes to actual non-routine incidents that required expert judgment or decision making (ibid). It is a theory-driven strategy that is 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 short description of the incident. Then a semi structured format is used to probe different aspects of the decision-making process. According to Klein et al. (1989), CDM has the following key characteristics:

- The CDM, like all critical incident techniques, focuses on non-routine cases. Incidents that are non-routine or difficult usually provide the richest 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 responses that can be objectively validated. Questions sometimes require the decision makers to reflect on their own strategies and bases for decisions.
- The CDM holds the middle ground between a totally unstructured approach, such as an ongoing verbal protocol, and one completely structured, such as an interview.

3.2 CDM 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:** We asked the participant to select an incident that presented a unique level of challenge.
2. **Obtain unstructured incident account:** Ask the participant to describe the incident from the start until the incident was judged to be under control.
3. **Construct incident timeline:** Reconstruct the account in the form of a timeline that established 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:** We used several probe types to gather more details on the decisions:
   a. **Cues**: What where 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?

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

3.3 Participants

In general, finding participants for research into cyber incident response is challenging and this is especially true for finding experienced CIR consultants. Worldwide there seems to be a shortage of cybersecurity talent and particularly experienced CIR consultants while the workload is large and even reported to be growing.[1] Consequently, it is difficult to find experienced CIR consultants that have time available to participate in research. That said, we attracted six experienced CIR consultants to participate in our research. Table 2 provides a list of the anonymized participants, employers, and their years of experience. CIR consultant 1 is employed by a CIR provider that works for a specific sector organization within the Netherlands. The other 5 CIR consultants that participated in our research are employed by an international CIR service provider.

Table 2: Participants, employers and years of experience in CIR

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

1 **https://www.forbes.com/sites/emilsayegh/2020/09/22/as-the-end-of-2020-approaches-the-cybersecurity-talent-drought-gets-worse/**

4 Results

In this chapter we present the results of our preliminary research.

4.1 Default strategy is to reduce uncertainty by investigating data and delaying decision-making

The interviews show that in general all respondents tend to seek as much certainty as possible before initiating any action to isolate or remove the threat from the environment. As CIR consultant 1 state: "The mindset of a cyber incident responder should always be: maybe I've missed something. You 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." In similar vein, CIR Consultant 3 note: "But of course the analysis phase must stop somewhere. I can never be 100% sure that I have identified everything. But you want to minimize the chance that you haven't found something before you act." And finally, CIR consultant 5: "You always want to do as many sweeps as possible before you start with the next phase."

Respondents bring forward one example in which immediate action might be required. In case of an ongoing ransomware attack, it is essential to quickly respond and isolate the infected systems as well as disconnect back-ups from the network. However, CIR consultants state that usually when they arrive at a client, the ransomware attack is already completed. Consequently, even in the case of a ransomware attack that encrypted the whole network, CIR consultants have a tendency to delay decision making and to buy time so they can investigate if there are alternative ways to recover the data. According to the respondents, an often-used strategy to buy time is to contact the attacker and initiate a negotiation process. In many cases, the respondents state, it is possible to negotiate about the ransom.

According to all respondents, one of the most difficult and recurring decisions during a data breach and particularly the incident remediation process is deciding when to move from investigation to eradication (i.e. removing an attacker from the environment and implement security improvements to inhibit the attacker from quickly regaining access to the environment). As CIR Consultant 2 puts it: "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 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 hinder the attacker's ability to progress towards its mission goals. Keyword being 'significantly'." All respondents agree 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 need to be used.

All respondents state that eradication should happen in the striking zone. CIR Consultant 3: "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 thorough 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 you start too late then there is a risk that the attacker can steal valuable information (which could have been prevented if you started eradication earlier). There is also a risk that the attacker becomes inactive, e.g. stops activities causing the investigation to lose track. If you remediate too early, then the attacker becomes aware of the investigation which allows him to change tactics, techniques, and procedures. This could result in the attacker becoming invisible or getting mad and attacking or disrupting even more systems.

In sum, the key question is how experienced CIR consultants decide when they are in the striking zone and how to do the eradication. The interviews indicate that all respondents apply a recognition-primed decision-making process.

The interviews show that all respondents use the simple match RPD model when making decisions about the striking zone. They state that when they arrive at a client to provide CIR services in case of a breach, the obvious option is usually to advise the client to use a so-called watch and learn strategy. CIR Consultant 6: "You have to make a call what to do when you arrive at 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 behaviour 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 he is being caught, then he can hide himself or start disrupting the network. You want to prevent that".

CIR Consultant 4 holds a similar opinion: "My initial strategy and advice to clients would always be to watch and learn 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 cannot see as we play what I call whack-a-mole."

4.2 Default strategy of delaying decision making does not always work well in every cyber breach

In some cases, as several CIR Consultants note, the obvious advice turned out to be wrong. CIR Consultant 5: "Three years ago I supported a client in Asia. It was a telco environment. The telco was breached. Attackers were in the environment for multiple years. When we found out, the primary reaction of the customer was to remove it. We had a fierce discussion. We advised them not to remove it yet. We wanted to get 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 used a web shell to download 500 gigs of data during the night. That was a really difficult call 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 watch and learn is the obvious option in the majority of incidents, there are some exceptions which could occur suddenly and require immediate eradication. The respondents state that there are several indicators that could signal an a-typical situation in which immediate eradication is the obvious 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 on a ransomware deployment mission and is about to decrypt the systems, then 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 quickly start eradicating are when you know that you 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 watch and learn to eradicate the most respondents use the concept of intuition. CIR Consultant 6: "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."

4.3 The default strategy to a ransomware attack: do not pay the ransom, unless...

CIR consultants indicate that they usually arrive at a client when the whole network is already encrypted. Consequently, in the majority of cases the incident is 'stable' in the sense that the damage has already been done. In these cases, the default decision-making strategy of reducing uncertainty and buying time is also applicable according to the respondents.

Another default strategy specifically related to ransomware attacks is concerned with paying the ransom. 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. 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, the initial advice would be not to pay the ransom and investigate whether the data could be retrieved in another way.

4.4 Paying the ransom is usually effective to retrieve data, but not always...

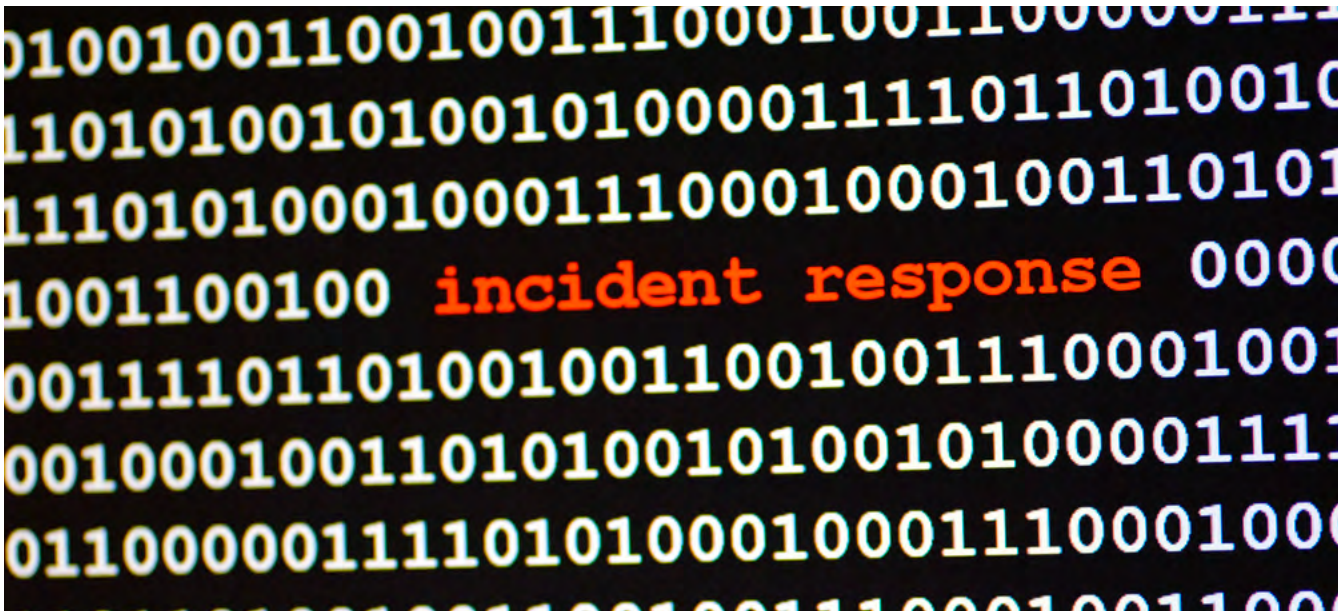
Some of the respondent's state that they do advice the client to pay a ransom in some particular instances. This is the case when the initial recognition of the situation is reassessed after all expectations about the situation are violated. For instance, when it appears to be impossible to restore the back-ups or finding workarounds that enable a quick recovery of the most important business processes. Or when 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."

According to the respondents, the obvious option in these 'hopeless' cases usually work out. 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. But in this case it worked out differently."

4.5 Default strategy is to provide incident response services until the job is finished

CIR Consultant 5 mentions that sometimes it feels difficult to stop incident response activities when it is unlikely that eradication will be successful. This is also known as the sunk-cost fallacy, a tendency to continue a chosen path once an investment in money, effort or time has been made.

CIR Consultant 5 explains: "I was hired by a customer in South Korea. A large gaming company was breached to steal signing certificates. The attacker was using a self-propagated backdoor which basically infected the binaries. You can see this as a virus component with a back door in it. We were chasing the attacker for months. It was basically playing whack-a-mole. We killed 10 infected systems and then next day 15 more popped-up. For us, the aim was to beat the attackers. At one day, we had a meeting with the COO. In hindsight, the COO made a difficult but wise decision. The COO said: Let's stop here. We will stop and build the company IT infrastructure from scratch."



4.6 Best practices based on CIR consultants' individual experiences

During the interviews, we also asked the respondents to provide best practices related to cyber incident response decision making. The list below provides a few best-practices that all were mentioned by at least 2 respondents. It should be noted that these best practices are based on CIR consultants own experiences and therefore are unique. Hence more research is needed to validate these best practices among a larger group of cyber incident responders.

Be aware of how group dynamics work and ensure a devil's advocate view: Several CIR Consultants mention that as CIR consultants usually work in teams. It is imperative to understand that group think could occur and advise to use a devil's advocate. Usually this is somebody not involved in the engagement or somebody that is less involved in the analysis such as the incident response coordinator.

Invest time to understand the specific business context: According to several CIR Consultants, having a decent understanding of the specific business context helps to make better decisions during the incident response process. As CIR Consultant 6 states: "When you start an engagement with a client, you need to learn the organization. I always ask for a company profile. How does the organization make money? What are the products and services? How do the business processes work? The more you understand the organization, the better you can support the client with making decisions and providing advice on the incident and crisis response." According to CIR Consultant 6, this good practice is also applicable to incident responders that work dedicated for an organization.

At the start of a new CIR assignment, take time to gather facts and buy time where possible: As noted in the previous paragraph, all CIR Consultants state that the incident analysis is the most critical phase in which sufficient time needs to be taken. As put forward by CIR Consultant 6: "You need to buy time. If you allow yourself to take more time at the start of the engagement, then it will turn out that you succeed earlier. So that would be my advice to anyone new in this field: take your time when you start with your assignment."

Ensure that team roles and responsibilities are clearly predefined: According to the majority of respondents, clearly defined roles and responsibilities are beneficial for CIR decision making. The CIR consultants explain that working following with fixed team structure and roles reduce the need for alignment and communication. This in turn results in better focus and more cognitive capacity available that can be used for CIR decision making. CIR Consultant 6: "A very clear division of tasks is crucial. You need to work according to pre-defined protocols, so the client and your colleagues know what they can expect from you." CIR Consultant 1 puts it like this: "A CIR team should have a routine of working together before starting an assignment. This might not always be possible, but it is beneficial in my experience."

Seek an effective working relation with the client and particularly the IT department: Some respondents state that CIR decision making is aided by safe climate in which consultants can speak up and in which there is a good working relation with the client. CIR Consultant 6: "Especially the relation with the client is underestimated. When we arrive at a client to support in cyber incident response, usually the IT department is in a panic because they may have made mistakes that could have caused the hack. Some IT staff might be afraid for the consequences. But we as CIR service provider need the IT department and want them to feel safe. They need to be able to tell us what could have happened. In addition, we do not want to take over responsibility from the IT department. We need to empower them. Therefore a safe and effective working climate with the client and particularly IT department is essential."

Take cultural differences and client's maturity level into account in the decision-making process: According to the CIR Consultants, the culture of the organization as well as the organizations maturity level have an impact on decision making. For instance, some cultures require more control and supervision than other cultures. This should be taken into account when making decisions on how to approach and lead a CIR engagement. CIR Consultant 4: "If I help a client in India, then I know that I should be more on top of it. In India they will always answer yes. Especially when the boss is in the same meeting. 'Are the back-ups secured?' They will answer yes, even if it is not the case. I know so many examples. Therefore, when you work for an Indian company, you have to write everything down. And only give them a few assignments and monitor them closely." CIR Consultant 2 states that maturity level of the client should also be taken into account: "Clients with a low maturity level…they need to be coached. This requires more time and effort, and hence you might want to expand the incident response team. Because the cognitive effort to complete the job remains the same, but you also have to teach the client."

5 Conclusion, discussion and recommendations

In this chapter we discuss the results, put them in a broader context, and present the conclusions of our preliminary research. We conclude with some recommendations for research and practice.

5.1 Conclusion and discussion

The main question of this research was: *What decision-making strategies do experienced CIR consultants use during challenging incidents and what are the implications for training and decision-aiding?*

Interviews with experienced CIR Consultants showed that they make use of the same decision-making model (RPD) as other operational experts (e.g. fire fighters, police officers, medical doctors) use when time pressure, uncertainty, and the stakes involved are high. This in itself, is an important finding as a lot of research has already been conducted on RPD and other NDM models containing many relevant suggestions of how the selection, education and training of experts can be improved.

The general conclusion of NDM research is that experts usually make adequate decisions based on (fast) recognition of the situation and applying the most obvious (default) response pattern that has worked in similar situations in the past. In exceptional situations, however, this way of recognition-primed decision making results in suboptimal decisions as experts are likely to miss conflicting cues once the situation is quickly recognized under pressure.

Understanding the default response pattern and the rare occasions in which this response pattern could be ineffective is therefore key for improving and aiding cyber incident response decision making.

The main conclusion of this preliminary investigation is that the default response pattern for CIR consultants during cyber breaches is to reduce uncertainty as much as possible by gathering and investigating data and thus delay decision making about eradication until the investigation is completed. According to the respondents, this strategy usually works well and provides the most assurance that the threat actor can be completely removed from the network. However, the majority of respondents could recall at least one case in which this strategy (in hindsight) resulted in unnecessary theft of data or damage.

Interestingly, this finding is strikingly different from other operational decision-making domains such as the military, police, and fire service in which there is a general tendency to act rapidly (see Groenendaal, 2015). Further research is required to understand this difference and to explore what these different domains could learn from each other regarding decision making.

5.2 Recommendations for future research

Conduct more research to specific NDM models within a CIR context. We recommend researchers conduct more research to the applicability of NDM models within a CIR context. In this research we focused on RPD, but there are models that could also be applied to gain a better understanding cyber incident response decision making.

Review NDM literature to identify improvement opportunities for the selection, education, and training: As we found that RPD is applicable to the CIR domain, we recommend researchers to explore how insights from RPD and more broadly NDM research could benefit the cyber incident response domain. Further research could look at how NDM insights as described in the literature can be used to improve the process of selecting, educating, and training cyber incident responders.

Investigate how team context influences decision making: 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.

5.3 Recommendations for CIR practice

Incorporate NDM into education and training of CIR professionals: Based on our preliminary research, we would recommend CIR practitioners to take notice of the NDM framework and particularly RPD as we have found many cases in which this decision-making strategy was used by experienced CIR Consultants. In training of CIR professionals, the default strategy as explained in this report should be explained including the exceptions in which this default strategy does not work well. CIR novices should also be taught how they can 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 even 'information addition' (e.g. Helsloot & Groenendaal, 2011) should be discussed as well.

Use insights from NDM 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. We call for more research that attempts to develop and test these types of decision aids for a cyber incident response context.

Reviewed literature

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.

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.

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.

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.

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.

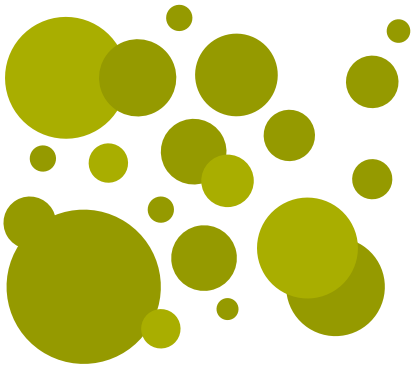
Simon, H. A. (1955). A behavioral model of rational choice. *The Quarterly Journal of Economics*, 69(1), 99-118.

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).

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.



Address and contact details

Johanna Westerdijkplein 75
2521 EN The Hague

thehagueuniversity.com

cybersecurity@hhs.nl