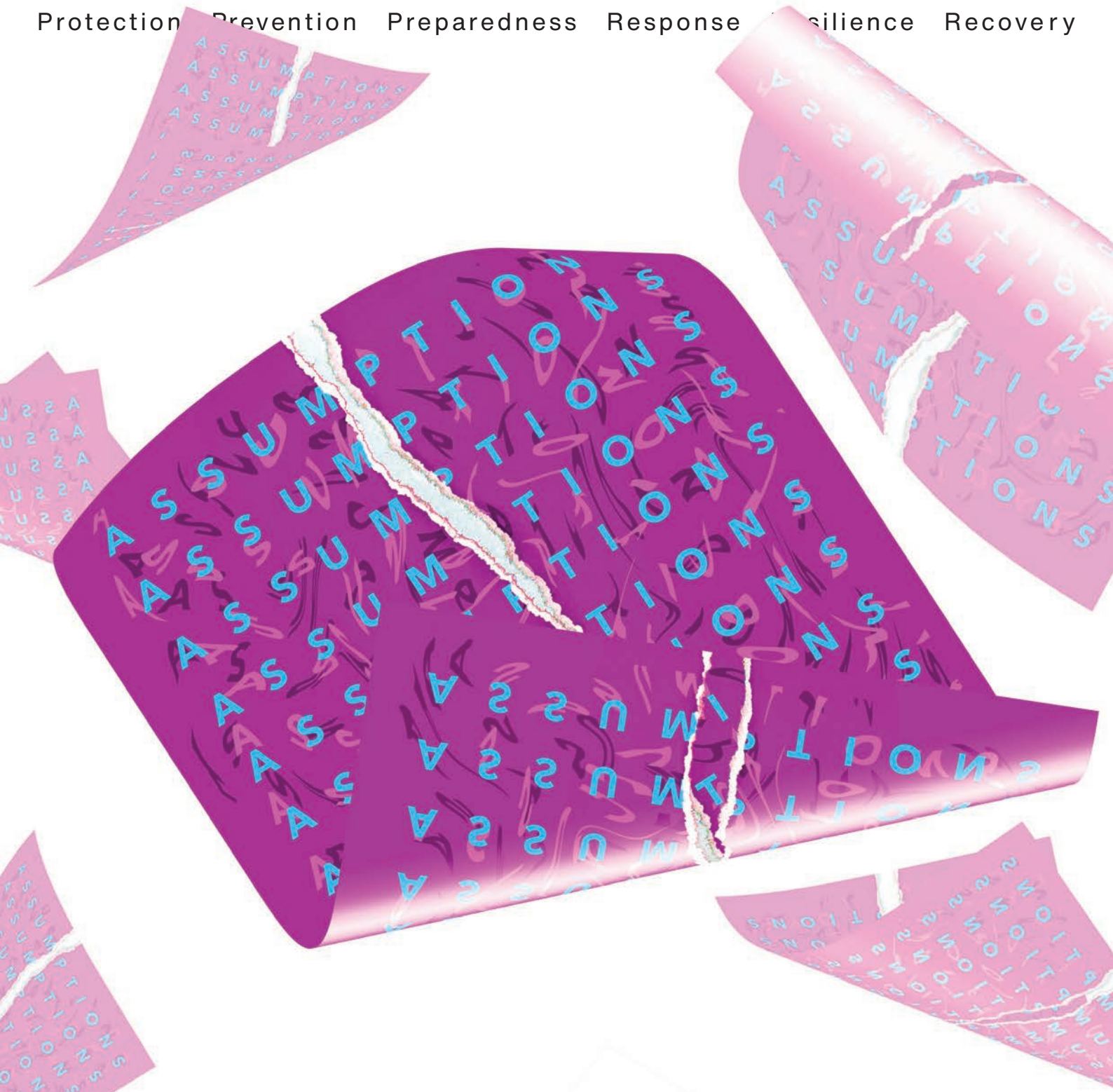
CRISIS RESPONSE

VOL:15 | ISSUE:3 | SEPTEMBER 2020 WWW.CRISIS-RESPONSE.COM JOURNAL

Protection Prevention Preparedness Response Resilience Recovery



RIP THEM UP AND START AGAIN?

Travel industry resilience | Covid-19 debate | Cybersecurity | Online tribalism & vigilantism | Frontline responder wellbeing | Karachi floods | Asteroids

Editor in Chief
Emily Hough
emily@crisis-response.com

Editorial Assistant
Claire Sanders
claire@crisis-response.com

Projects Development Manager
Derya Kemmis
derya@crisis-response.com

Design & Production
Chris Pettican
chris@layoutdesigner.co.uk

News and Blog research
Lina Kolesnikova
lina@crisis-response.com

Web Support
Neil Moultrie

Subscriptions
Crisis Response Journal is published quarterly; it is available by subscription in hard copy or digital.
subs@crisis-response.com

Published by Crisis Management Limited, Sondes Place Farm, Westcott Road, Dorking RH4 3EB, UK

Printed in England by The Manson Group, UK
ISSN 1745-8633

www.crisis-response.com
Crisis Response Journal on LinkedIn
Twitter @editorialcrj

contents

Human-centred response: p16

Jazzia | 123rf

Cyber espionage: p50

Sergio Ingravalle | Ikon Images

Cover story: Is it time to rip up our assumptions?
Cover image: Gracie Broom

Terrorism & vigilantism: p64

Gracie Broom

The Great Reset: p96

Anan Punyod | 123rf

comment

This edition of the *CRJ* is about challenging assumptions, unpicking the strands of the Covid-19 pandemic and its multiple cascading consequences, all the while being mindful of how they are conflating with other disasters and emergencies, such as the storms, other extreme weather and wildfires sweeping across the world.

Many cosy assumptions about emergency preparedness systems, society, security and international relations have clearly been misguided and, in part, this stems from a historical lack of emphasis on preparedness and mitigation in favour of post-crisis response. On p28 Eric McNulty notes: "The ever greater demands we place on responders are the result of design failures in our institutions and communities," asking, "How often have you seen ... honorifics bestowed on those who labour on mitigation, preparedness and recovery?"

This leads us to the status of the complex horizontal and vertical relationships between governments, emergency preparedness experts, responders and, most importantly, the public. Assumptions are all too often being made about public involvement in – and experience of – emergencies, as emphasised by David Wales on p16.

When systems are found wanting and citizens don't feel that their needs are being addressed or recognised by authorities, unrest and dissent can proliferate. Starting on p60, *CRJ* looks at some of the manifestations of such unrest, from lockdown tribalism to overzealous digital behaviour. These trends affect us all – business, emergency planners, responders, governments, communities and individuals – and Jennifer Hesterman provides a sobering reminder of what happens when online crime, terror and vigilantism spill over into the real world (p64). This is backed up by the heightened vulnerabilities highlighted by authors in our cyber feature (p40).

CRJ is not for tearing down systems that work, nor does it advocate the indiscriminate ripping up of assumptions. But failure to ask questions and debate the more difficult subjects that have been skirted around for many years, can only lead to crippling atrophy.

Leading a cyber incident response team

Jelle Groenendaal and **Ira Helsloot** present a model of cyber incident command that aims to support leaders by providing practical and applicable insights into decision-making under challenging conditions

In the case of a major cyber incident such as a distributed denial of service (DDoS) attack with business impact, multiple systems compromised by malicious software or a data breach containing sensitive information, organisations usually deploy a cyber incident response team (CIRT).

CIRTs have to make important, sometimes even critical decisions in challenging circumstances involving time pressures and uncertainties. Leading a CIRT during cyber incidents or crises – termed cyber incident command – requires a good deal of crisis management capacity from the team leader.

A CIRT is responsible for various tasks such as: Incident response – identification, containment, eradication and recovery; forensics – gathering and analysis of crime-related evidence following incidents; and incident management – co-ordination of incident response and impact mitigation. A CIRT may include both internal and external personnel and the composition may differ, based on the nature of the incident. The core team usually consists of cyber security and IT staff. The extended team may include other capabilities as well, such as other IT domains, communications, business and legal.

Challenging decisions need to be made about the scope of the investigation, which hypotheses are examined and which are not, or the actions to contain the incident, including what IP ranges are blocked to stop a DDoS attack. Choices might also include measures to mitigate the impact, such as which external communication strategy is used. Furthermore, CIRTs have to balance different, or sometimes conflicting, interests.

Cyber incident command can be defined as the process of making decisions about the response to, and management of, cybersecurity incidents and ensuring that these decisions are carried out accordingly. CIRT members – cybersecurity engineers, forensic investigators, threat managers and so on – are often experienced professionals. Naturalistic decision-making (NDM) research into decision-making under challenging conditions has shown that in the majority of cases, professionals do not need close supervision as they are task-mature and able to make appropriate decisions. However, NDM research has also demonstrated that professionals are susceptible to decision-making flaws in certain cases. In these instances, cyber incident command is needed to prevent these flaws or limit their impact.

The FADCM model of cyber incident command has been designed for incident commanders who need to make critical decisions under challenging conditions, and then ensure that they are carried out. The model was originally applied to frontline fire and police commanders, but its generic design allows application to other domains.

For each of the five steps of the FADCM model – fact finding; analysis; decision-making; communication; and monitoring – insights from NDM and other relevant research are used to aid cyber incident command.

In the first fact finding stage, cyber incident commanders have to amass relevant information from the environment. Two core insights from different streams of research play a role here. The first is that professionals make decisions based on their perception of reality, described in NDM literature as situation awareness. This involves the completeness and accuracy of an individual's or group's perception of a situation and the extent to which they can predict the consequences for the near future.

Recognition primed decision-making

In order to achieve situation awareness, professionals have to carry out a situation assessment. In this process, professionals use their knowledge and experience to create a perception of reality that they use to validate any new information received from the environment. Recognition primed decision-making (RPD), a core NDM theory, plays a prominent part here; when professionals recognise a pattern in their environment, when they know what solution in the past produced a satisfactory outcome and are subject to great time pressure and uncertainty, they will tend to opt for that solution immediately.

However, this can also mean that despite accurate knowledge and experience, professionals can still make wrong decisions if their perception of reality does not correspond to the actual situation, underlining the importance of developing a high level of situation awareness. So fact finding is an important element here.

The practical implications for cyber incident commanders are that they should actively search for information and use it to validate their perception of reality in the light of the current situation. In addition,

Gracie Broom

Only after a hint from a hired cyber incident responder still on their way to the municipality, did the IT department discover that other employees had also received the phishing e-mail

they must proactively validate the accuracy of information they receive from CIRT members and other stakeholders and not rely solely on the information they receive.

In one incident, an employee of a municipality in the Netherlands accidentally downloaded malware on his computer after clicking a link in a phishing email. The employee did not trust the link and reported the suspicious email to the IT department, which uncovered the malware and found that data had been sent from the employee's computer to a server that had probably been compromised.

The IT department removed the malware and reported that the incident had been resolved. Only after a hint from a hired cyber incident responder still on their way to the municipality, did the IT department discover that other employees had also received the phishing e-mail. An investigation revealed that several workstations were infected with malware and had sent data to various compromised websites.

This example shows why it is important not to rely solely on information received, such as: "The incident is resolved," but to ask actively for more facts, posing questions such as: "Have other employees received a similar phishing message?"

The second core insight from psychological research, however, is that people's attention and working memory are limited. Only limited amounts of information can be processed and, for the most part, people take notice of the information that they are searching for and tend to overlook that which they are not expecting. Moreover, NDM research shows that people who opt for quantity of information – broad focus – as opposed to quality of information, generally possess less situation awareness, which can lead to fewer satisfactory decisions and, consequently, more mistakes.

The practical implications of these insights for cyber incident commanders is that they should be restricted in the number of tasks they perform at one time, owing to an inherent limited cognitive capacity to gather and process the information pertaining to each task.

The second step of FADCM is to perform an analysis of the situation. This involves identifying the problem and its significance for the present and the immediate future. Again, two core insights are relevant here.

The first insight from psychological research is that people have access to two different modes of thinking: System One and System Two. The first is decision-making based on RPD. Although this is by far the more dominant system, people do not only make decisions based on experience and recognition. System Two makes use of people's ability to reason and is able to correct any flaws that are made by System One.

As noted earlier, under high levels of time pressure, CIRT members are likely to make decisions based on System One. In practice, this means that cyber incident commanders must consciously take the time to engage System Two so as not to make the same errors as CIRT members.

Delaying a decision by 'buying' time is one of the most important methods of strengthening reasoning ability. The practical implication for cyber incident commanders is simply that they should subject a decision to a final review before issuing the associated order.

The second NDM insight is that System Two is not only influenced by time pressure, but also by task load. When cyber incident commanders are subject to a heavy cognitive load, for example when carrying out various tasks simultaneously, performing complex tasks or processing large amounts of information at the same time, there is less cognitive capacity available to analyse the situation consciously. Therefore, it is evident that cyber incident commanders should concentrate on the most critical task and organise backup for those that can no longer be carried out.

This was a case in point in the example we mentioned earlier, where the hired cyber incident responder formed a CIRT, together with representatives from the IT department and the data owner. As the technical forensic expertise within the team was limited, the hired cyber incident responder became deeply involved with the technical investigation, finding out what data had been leaked.

As a result, apparently everyone had forgotten to lift the blockade on the outgoing internet line, resulting in four hours of unnecessary business impact. In retrospect, the hired cyber incident responder said that it would have been better if he had appointed somebody else to look after the business impact, because he was so deeply involved in the technical work.

The third step of FADCM is decision-making, ie ensuring that orders are carried out correctly after a decision has been made. This requires considerable effort on the part of cyber incident commanders, particularly when it involves decisions that could be interpreted by CIRT members as being counterintuitive.

One limitation of RPD is that the majority of actions performed by CIRT members are carried out on autopilot and involve skill-based behaviour. Studies have shown that skill and rule-based behaviour – the conscious application of learned rules – cannot easily be changed during incidents and therefore require considerable supervision on the part of cyber incident commanders. The term 'supervision' refers to communication and monitoring, which will be addressed later in the article.

As a result, it is advised that cyber incident commanders should consciously consider whether a decision could be experienced as counterintuitive by CIRT members and restrict the number of decisions made; not only in order to limit their own task load, but primarily to prevent excessive pressure on cyber incident responders.

Referring to the aforementioned case study in the Netherlands, the municipality wanted to know what it should report to the local privacy authority and the CIRT worked hard to find out what data had been compromised. It appeared to be difficult for the CIRT to identify what data was involved and whether it had actually been shared with the server. After consultation with one of the hired cyber incident responder's colleagues, the municipality decided to stop further investigations because it would be too expensive to conduct further examination while the return of investment was questionable.

Afterwards, during the evaluation, the CIRT said that it felt counterintuitive to stop the investigation at that time, even though it now agreed with the decision.

At the fourth FADCM step, communication, a decision has to be translated into an order and delivered to the CIRT members. The issue is how to do this in the most efficient and effective manner.

Communication has traditionally been regarded as a model comprising a transmitter and a receiver, which send each other a message and feedback. Research has shown increasingly that, in regard to more complex communication between people whose purpose it is to influence one another, this is a wishful model. In the type of complex communication at hand, people do not receive 'messages' but interpret information according to their own frame of reference, which consists of values, beliefs, goals and cultural aspects.

Let's revisit the case study where the municipality's chair of the strategic crisis management team informed the CIRT about the decision to stop the inquiry.

He explained how the team arrived at the decision and how several stakes had been balanced, including minimising further financial costs and the operational impact of the change freeze that had been established. He explicitly ordered the CIRT to stop the investigation, to file a report with the police and to write an internal evaluation.

Well-formulated orders

It is clear that cyber incident commanders should formulate an order carefully. On the basis of NDM research, three elements of a well-formulated order can be distinguished. The order should first clarify the intended recipient, the person who is to carry out the order. Second, it must outline the approach and conditions under which the order is to be carried out, such as when, using which resources, and any special areas of attention. Third, it must identify the goal, exploring why it is important and how the task will contribute to achieving it. Cyber incident commanders should actively verify whether CIRT members have understood the orders they have received.

After the order to stop the investigation, the CIRT still did not know whether the attacker had accessed the data that had been sent to the server. So, the CIRT reached out to the owner of the compromised server and requested the logs in order to conduct further investigations.

The chair of the strategic crisis management team became aware of this when he visited the CIRT and intervened to forbid this action. This leads us to the fifth, and final step, which is monitoring.

During this phase, cyber incident commanders must ensure the correct execution of the communicated order. The majority of empirical research into communication during emergency situations shows that orders are often misunderstood or simply forgotten by subordinates. Particularly in the case of non-routine orders, explicit monitoring seems to be vital to ensure that the orders are carried out in a correct and timely fashion.

There are valid examples of such explicit monitoring in action to be found in firefighting operations. The practical implication for cyber incident commanders is to monitor all orders until they have been carried out by CIRT members. In the event of a shortage of time, this task should be delegated to a colleague cyber incident commander. CRJ

Authors

JELLE GROENENDAAL *is research director Risk Management and Cybersecurity at the Hague University of Applied Sciences, the Netherlands, and independent consultant risk and crisis management*

IRA HELSLOOT *is professor, Governance of Safety and Security at the Radboud University Nijmegen, the Netherlands, and chairman of Crisislab, a research foundation specialised in safety, risk and crisis management*

CRISIS RESPONSE

JOURNAL | WEBSITE | EVENTS | SOCIAL MEDIA | NETWORKING | BUSINESS DEVELOPMENT

MULTIPLY

the force of your business

Open doors to the people you really want to meet. **Influence your market** and **build your brand awareness**, across the global crisis and emergency response fields.

Key Network Partnership:

We call them Key Network Partnerships. Because you're not just becoming a partner of ours - but leveraging access to our entire global network. It's about connecting you with the right decision-makers. We open doors and introduce you to the right people, with the power to transform the next phase of your business development. And it's about intelligently marketing your business, to your target audience, across our global platforms. Extending your reach, increasing your exposure and driving your brand awareness.

Call CRJ today about becoming a Key Network Partner on **+44 (0)203 488 2654**

PROTECTION | PREVENTION | PREPAREDNESS | RESPONSE | RESILIENCE | RECOVERY

www.crisis-response.com

CRISIS RESPONSE

JOURNAL

PROTECTION | PREVENTION | PREPAREDNESS | RESPONSE | RESILIENCE | RECOVERY

SUBSCRIBE NOW

visit **www.crisis-response.com** for rates and special offers

Authoritative global coverage of all aspects of security, risk, crisis management, humanitarian response, business continuity planning, resilience, management, leadership, technology and emerging trends

PRINT | ONLINE | DIGITAL