

CRISIS▶RESPONSE

VOL:15 | ISSUE:1 | MARCH 2020

WWW.CRISIS-RESPONSE.COM

JOURNAL

Protection Prevention Preparedness Response Resilience Recovery



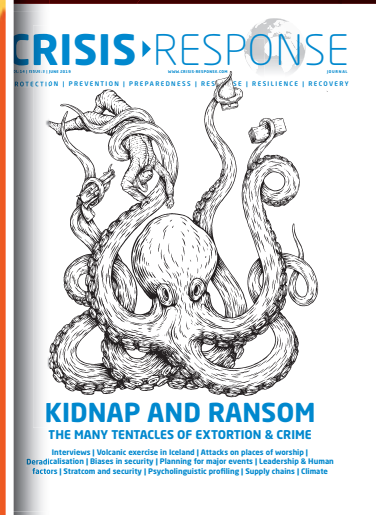
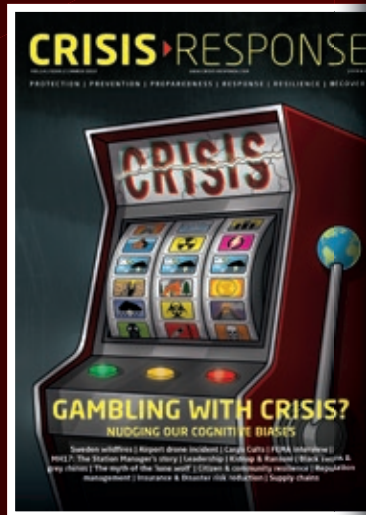
FRACTURES

Societal | Grey Rhinos | Covid-19 | Brexit |
Earthquakes | Conflict & Peacebuilding |
Cyber Threats | DRIVER+ Final Results | Bushfires

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

contents

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@crisis-response.com

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, digital and online
subs@crisis-response.com

Published by Crisis Management Limited, Soudes Place Farm, Westcott Road, Dorking RH4 3EB, UK
COPYRIGHT Crisis Management Limited 2020.
Articles published may not be reproduced in any form without prior written permission.
Printed in England by The Manson Group, UK
ISSN 1745-8633

 www.crisis-response.com

 join the CR/LinkedIn group

 follow us on twitter @editorialcrj

News	4	Insarag anniversary	40
Comment		Lucien Jaggi describes the 30-year achievements of the International Search and Rescue Advisory Group	
The 'wrong people' around the table	8	Business continuity	
Rob McAlister says the more cognitive diverse a team's composition, the better it can provide solutions		Much more than cyber	42
A metaphor for our times	12	Concentrating solely on cyber threats at the expense of more traditional problems is not a good way forward, contends Lyndon Bird	
Emily Hough speaks to Michele Wucker, who introduced the Grey Rhino concept to the world		The role of ERM	46
Mitigating disasters in a fractured world ..	16	Hans Læssøe debates the approach to – and value of – enterprise risk management in today's ambiguous, volatile and complex world	
Today's threat landscape is increasingly cross-border, undeterred by traditional lines of sovereignty. It is also largely asymmetric, says Amy Pope		Creating resilience from turmoil	48
Australian bushfires		Brexit highlights several factors that we can learn from and make the necessary changes to take society to the next level, according to Adrian Clements	
Fire Service response	20	Preparing a frontline service for Brexit	50
Fire Chief Mark Jones describes the challenges that the bushfires presented in South Australia		Alex Darling describes how a UK ambulance service has prepared to mitigate the potentially adverse effects of Brexit	
Operation Bushfire Assist	24	Leadership and Covid-19	52
Senator the Hon Linda Reynolds, Minister for Defence, tells Emily Hough how Australia's armed forces are helping with response and recovery		The actions of leaders can make the difference between panic and calm concern, says Eric McNulty	
When can we talk frankly?	26	Performing under pressure	54
Christine Jessup contends that we all need to play our part in adapting to climate change for our survival		Anna-Maria Rochester describes lessons from hostage negotiators that apply to anyone who has to perform in high stress situations	
A total rethink: Our moral responsibility ...	30	A special focus on DRIVER+	58
Greg Mullins, former Commissioner of Fire and Rescue for New South Wales, shares his thoughts on the recent bushfires with Christine Jessup		We present a special feature on the DRIVER+ project, which aims to boost crisis management, innovation, operational effectiveness and networking. Here, we look at its achievements and legacy	
Frontline response		Communities	
Albania earthquake	34	A centre of hope in Cambodia	66
John Doone reports on Kosovo's response when Albania reached out for help from its neighbours		Nigel Ellway describes a new victim support partnership being developed in Cambodia	
A peek into the future with the SCDF	36		
Emily Hough learns more about the Singapore Civil Defence Force's trailblazing technology from Commissioner Eric Yap			

Australia's bushfires p20



Commonwealth of Australia 2020

DRIVER+ project p58



DRIVER+

comment

A new peacebuilding model 70

Larissa Sotieva and Juliet Schofield argue for a transformative model of peacebuilding

Cultural understanding 74

Awareness of other cultures is a vital component in managing crises, explains Matt Minshall

Citizens: Vital co-actors 78

Governor Gilles Mahieu announces collaborative agreements as part of the Belgian Province of Walloon Brabant's efforts to encourage citizens associations in crisis preparedness

Unprompted acts of kindness 80

When it comes to spontaneous volunteers, Ali Malvern says that professionals must shift their mindset

Preparedness for children 82

Rob Fagan argues the case for instilling first aid and emergency preparedness in our children

Testing in the Caribbean 84

Alois Hirschmugl, Anna Lena Huhn and Albrecht Beck describe an exercise with thousands of participants

How VR enhances humanitarian learning . 86

Atish Gonsalves and Anne Garçon outline exciting developments, especially in terms of safeguarding and building empathy

Security

The dangers in our digital shadows 88

Ghonche Alavi offers advice on how to minimise online threats

Leaders on the cyber battlefield 90

Jeffrey Crump explores practical ways to conduct cyber crisis management training

Cyber threats and emergency services..... 92

Beatriz Peon provides several examples of how emergency public services have fallen victim to cyberattacks

Counterterrorism in cities 94

Terrorism is a global, networked and persistent threat, so counterterrorism must also be global, networked and persistent. Alex Townsend-Drake elaborates

Cities & society

The tall buildings challenge 96

It is expected that the one-kilometre-high barrier for buildings will be broken soon. This raises the stakes in emergency preparedness, according to Russ Timpson

Tall buildings and high reliability 98

Everyone involved in high-rise buildings should look to high reliability organisations for inspiration, says Shane McMahon

Health systems – a critical element 100

A look at how the WHO is working with the Kyrgyz Government to strengthen emergency preparedness and response

Delivering a different approach 104

Ruth Wozencroft explores whether it is necessary to redesign or redevelop out-of-date hospitals

Tech for good

The global impact of drones 106

Charles Werner lists the numerous ways that drones are being used to save lives and protect communities

Crisis mapping 108

It is important that we understand the relationship between the formal humanitarian sector and digital volunteers, explains Doug Specht

Regulars

Events 110

HNPW review 112

Indonesia conference 113

Frontline 114

Preparing and helping children to deal with major incidents is the foundation of ensuring resilient communities. Claire Sanders speaks to Heather Beal, President and CEO of Blocks

“Today’s biggest problems defy simple, short-sighted solutions,” commented

Ambassador (Ret) David Carden in the *South China Post* on February 19. Although Carden was referring to the global response in the face of Covid-19, his thoughts on complex adaptive systems are applicable to the whole gamut of crisis risks.

On p4 of this edition of *CRJ*, we discuss the *Global Risks Report 2020*, which forecasts a year of increased domestic and international divisions. It says: “Systems-level thinking is required to confront looming geopolitical and environmental risks and threats that may otherwise fall under the radar.” On p12 Michele Wucker points to the need for greater systems-level thinking when considering far reaching global challenges such as climate.

Wucker also highlights the benefits in terms of resilience in societies where people do not just consider themselves as individuals, but as part of a larger group.

“Thinking holistically is part of what transformation research is all about. We can’t all be running around doing our own thing individually,” notes Professor Wilson of Ohio State’s School of Environmental and Natural Resources, in a call for less focus on individuals and more work to inspire collective action in preparedness for climate threats (p4).

As Amy Pope says on p16: “No single government, or even a multilateral institution, is equipped to respond to any major disaster alone. In a world where major governments are choosing their own countries first, we are fighting disasters with one arm tied behind our backs.”

Pope continues: “Ultimately, we need to rethink the way that societies engage collectively. In the absence of leadership from governments, there is an opportunity for corporations, non-governmental actors and individuals to influence the debate, push for reform, build coalitions and fill the gaps...”

So in this fractured landscape, who is stepping in to fill the yawning gap in trust and governance? Interestingly, the *2020 Edelman Trust Barometer* (p6) notes that: “Business has leapt into the void left by populist and partisan government.” Other factors in achieving a holistic, co-operative approach include cognitive diversity (p8), cultural understanding (p74), citizens themselves (p78) and spontaneous volunteers (p80).

Fractures can be healed. Admittedly, this can be a painful process, but it does appear that a fundamental change in thinking is now imperative. We *all* have a role to play in this.



SCDF trailblazing p36



SCDF

Digital volunteers p108



HOT | Chris Morgan

Creating leaders on the cyber battlefield

What leadership skills and qualities are needed when dealing with a cyber incident?

Jeffrey Crump explores practical ways to conduct effective and comprehensive cyber crisis management training



uch has been written regarding decision-making during a crisis. However, very little has been published on the different influences and thought processes that affect crisis decision-

making, and even less has actually been done to help crisis leaders become better at decision-making when under pressure. Let us explore these facets to determine how organisations can reduce risk and increase organisational resilience by outfitting leadership with the mental muscle memory needed to lead effectively during a crisis.

Preparing leaders for future crises presents many challenges to trainers. Leaders must be able to take effective and sometimes independent action across a diverse range of possible situations. They must be able to make quick decisions under complex, uncertain and very fluid conditions. With our reliance on technology, nowhere have these conditions been more dynamic than in the cyber battlegrounds, where organisations and governments face malicious threat actors ranging from beginner script kiddies practising their hacking skills, to well-organised, co-ordinated hacktivists seeking to punish those who disagree with their cause.

This extends to even more advanced persistent threats (APTs) that may be backed by a global financially-motivated cybercrime ring, or nation states seeking to steal valuable intellectual property or to gain a foothold in an adversary's critical industrial control systems that supply water and energy.

Crisis planning is essential, but these cyber-related risks mean that cyber crisis management planning has emerged as an important pathway to risk reduction. From a high level, organisations must develop a cyber crisis management plan (CCMP). This should extend well beyond the traditional information technology incident response plan and deliver a cross-organisational plan that integrates the functional incident response plans of key functions such as IT, privacy, legal, marketing, physical security, core business units and so on.

Like other crisis management plans, developing and executing tabletop exercises are essential to validating and optimising the functional incident response plans and the overarching, integrated CCMP. It is during these exercises where crisis leadership skills, or lack thereof, become apparent. However, owing to personal traits and organisational influences, opportunities to make crisis leaders better often get swept under the carpet. We

must recognise that tabletop exercises are designed to validate and test the plan's activities, inter-relationships, and logistics; they are not designed to be safe spaces for crisis leaders to cut their teeth. A crisis leader who walks away from a CCMP tabletop exercise humiliated and embarrassed by their own performance is a victim of the organisation's lack of overall crisis training.

We know that there is a multitude of personal and professional influential factors to be considered. The best place to start when developing high-performing, confident cyber crisis leaders is by building an unbiased personality and performance profile. Leadership assessments can provide a unique perspective of a leader's performance capabilities, challenges and underlying motivators. This information can be used as input to develop a cyber crisis leadership strengths, weaknesses, opportunities, threats (SWOT) analysis, which the leader and trainer use to drive improvements.

When we have this information, we can begin the process of preparing leaders to manage crises effectively in a training environment that is safe, one that allows a crisis leader to practise without critical judgement. Coupled with physiological data points such as galvanic skin response, pulse rate, and eye tracking collected during mock situations, it can paint a high-resolution crisis leadership image.

Following a typical tabletop exercise, it is common to complete an after-action report (AAR), which documents the conditions and results of a cyber crisis incident and war game. The AAR should include an executive summary, overview of the exercise scenario and objectives, approach taken by the exercise lead and participants' level of engagement, attack storyline and observed reactions, and areas identified for improvement, including details regarding the gaps in the functional incident response plans. Where this wrap-up activity typically falls short is in not delivering one-on-one leadership performance feedback, which can result in the leader assuming their processes and performance were optimal, despite this possibly being the opposite of the truth. In other words, it can reinforce sub-optimal traits.

On a typical business day, organisational leaders are tasked with making a variety of decisions. During these times the leader employs a classical approach to decision-making by considering a range of options, weighing each one, then selecting the option that best serves the situation. What some people fail to realise is

that the decision-making process used under low-stress conditions is very different from high-stress, time-constrained, context-free, naturalistic conditions. Hence, a leader who has a reputation for making sound strategic decisions may falter when faced with high-pressure demands. Under these heightened conditions, the leader must be able to make fast, accurate assessments of the decision situation under uncertain and rapidly changing conditions, with severe time constraints.

Garbage in, garbage out

To be successful as a cyber crisis leader, or any crisis leader, requires strong situational awareness. Such leaders need an ability to perceive and comprehend large volumes of information in a short amount of time and then make sound decisions. These cognitive processes require identification of the various meaningful elements in the environment, understanding what these elements are, and translating this into an understanding of possible future events. Things often go wrong for organisations when the crisis leader makes the correct decision based on perception, but faulty situational awareness leads to incorrect perceptions. In the data world, this is called 'garbage in, garbage out'.

In order to gain the right situational awareness, thought processes have to shift from a classical to a naturalistic approach. During a crisis, the leader must have gained the skills to achieve situational awareness to identify the key situational components, because these significantly shape the crisis decision-making strategy. We already know that tabletop exercises are not the place for this training, so

specialised cyber crisis leadership boot camps are needed to close this significant training gap. However, these can be costly and disruptive to day-to-day operations.

So where can we find an alternative training environment that is more affordable and has less negative operational impact than flying an organisation's cyber crisis management and response leadership team members to an offsite facility for several days; one that is flexible enough to be configured for a variety of exercise scenarios; which provides a safe space for leaders to fail forward; and employs personal, one-on-one performance feedback? Based on research conducted by the US Army Research Institute for the Behavioral and Social Sciences, that place is virtual reality (VR).

In the two decades since the Army's seminal work proving the effectiveness of using virtual environments to train real world decision-making skills under high-stress conditions, VR has come into the mainstream as a cost-effective, flexible and readily available training platform. For many organisations, the use of VR for training will be a new experience, which may slow, but not prevent, adoption.

Virtual training environments are an exciting and innovative solution for a significant risk facing most organisations – ineffective cyber crisis leadership. As clichéd as it sounds, reducing cyber risk and increasing organisational resilience requires a combination of people, process and technology, but begins with building, testing and validating a solid cyber crisis management plan, and ensuring that those tasked with leading the crisis response are trained and skilled to do just that.

Author



JEFFREY CRUMP is the principal consultant at Cyber Crisis Response and author of *Cyber Crisis Management Planning: How to reduce cyber risk and increase organisational resilience*



www.cybercrisisresponse.com



Comickstocks | 123rf

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



Strategic Solutions for Global Issues



CRISIS MANAGEMENT
LIMITED

Our experienced multi-national team bring years of expertise in all aspects of Resilience, Crisis Management, Policing and Security services, making Crisis Management Limited a key resource for any level of related work, whether at a local, national or international level across public, private or voluntary sectors. We do not believe in 'off the shelf' solutions but seek to work with all clients to ensure bespoke services that meet clients' needs and expectations. No projects are too small or too large.

Our multi-disciplined team has vast experience across all sectors and continents. Our experts have the flexibility to provide support at State or Government level for long term work, as well as bespoke niche work on a smaller scale and for short periods. The can-do approach of our team means that we can provide support at short notice if required.

- › International Experience
- › Bespoke Service
- › Flexibility
- › Customer Focus
- › Communication Expertise
- › Breadth of experience

www.crisismanagementlimited.com

info@crisismanagementlimited.com