BIG DATA: AT THE HEART OF EVERYTHING

PLUS: Landslide Search & Rescue; Wildfires in South Africa; Humanitarian-civil-military co-operation; Cyber security; Urban resilience; Safer cities; Pakistan school shootings; France terror attacks
Now in its tenth year

Read Crisis Response Journal in print, on Tablet or online

Individual, Institutional (including unlimited digital downloads). Digital only and student rates available

Subscribe now: Contact us on +44 (0) 208 1669 1690 Or email subs@crisis-response.com
**News** ................................................................. 4

**Comment**

Is humanity the collateral damage of terror? .......................... 8

Governments and societies should react in a measured manner to incidents such as the Charlie Hebdo attacks in France, or the Martin Place siege in Australia, says Christine Jessup

**Women and violent extremism** .................................. 12

Mehdi Knani examines measures to prevent and counter violent radicalisation among women and girls

**Terror & Security**

January attacks in France ............................................. 14

Christophe Libeau describes the operational, tactical and strategic operations during the Charlie Hebdo attacks and subsequent hostage-takings

**Hardening businesses against terrorism** ......................... 16

Chris Phillips describes simple actions all businesses should be taking to protect themselves and their staff

**SMEs also need to protect themselves** ......................... 18

How can operators of smaller soft targets protect themselves from attack? Lina Kolesnikova investigates

**Pakistan school attack** .............................................. 20

Luavut Zahid reports from Peshawar, where terrorists gunned down 145 pupils and staff in a military school

**Asymmetric attacks at sea** ......................................... 22

Dave Sloggett reflects on the growing levels of instability in the maritime domain

**Disasters & urban resilience**

Wildfires in South Africa ............................................. 24

Firefighters faced one of the worst blazes ever experienced around the Cape Peninsula, writes Hilary Phillips

**SAR after US mudslide** ............................................. 26

Thomas J Richardson shares a USAR team’s experience in a very different environment to its usual operations

**Resilience starts with people** ...................................... 32

Where poverty is widespread and resources scarce, social capital is more essential than ever, says Katrina Borromeo

**Co-operation: A case study** ...................................... 33

Jay Levinson details story behind the headlines in the Middle East that gives hope to those who wish for a future of tranquillity and co-operation

**Collective intelligence** .............................................. 34

Alejandro Salazar Ortuño describes a Spanish initiative to create smart and resilient communities

**Big data, cyber security**

**Making sense of big data** .......................................... 36

A galaxy of user-generated data points is providing a near-unimaginable quantity of data that can improve disaster preparedness and response. But first there are some problems to overcome, warn Ian Portelli, Ramin Bajoghli, Megan Mantaro and Amanda Horowitz

**Cyber-consequences** .............................................. 39

An effective and credible response to cyber attacks could demand a diverse, agile and eclectic approach to emergency response, according to Andy Marshall

**South Africa wildfires** p24

**Cyber threats: protection advice** p44
Cyber threats: The ever-changing spectre
Cyber threats are dynamic and asymmetric, requiring a change in organisational approach, says Chris Morgan

42

Humanitarian sector and cyber threats
David Prior warns that most cyber attackers – nation state or criminal alike – do not care that you are a humanitarian or rescue operation

44

Planning for the breach
It is a matter of when, not if, your systems are breached, says Regina Phelps. Exercise and test your response

48

International co-operation
It is time to tighten up collaboration, according to Annemarie Zielstra, Eric Luijff and Hanneke Duijnhoven

50

Interview
Emily Hough talks to Todd Rosenblum, the Pentagon’s former Assistant Secretary for Homeland Defence

52

Experiences of the military and disaster
Alois Hirschmugl shares his thoughts and experience

54

Shaping humanitarian-civil co-operation
Eugene Gepte emphasises the importance of both sectors maintaining their respective identities

56

An ECHO perspective
Vera Mazzara outlines EU civil-military engagement

59

Improving collaboration
Heiko Herkel describes the work of the Civil Military Co-operation Centre of Excellence

60

NATO’s civil emergency planning
Günther Bretschneider explains how NATO works with others to ensure the most effective use of civil resources in an emergency

64

In Depth
A look towards 2050
Time is running out if we are to build truly resilient cities for the future, according to Brett Lovegrove

66

ICDO Part III
A look at civil defence organisation in Jordan

70

Staff rotation in a crisis
Marjan Örnenstein lists the factors that affect deployment times on a crisis team at management level

72

Situational awareness
Friedrich Steinhäusler introduces the first part of a series describing a system that incorporates UAVs, a computer-based expert system and 3-D modelling to provide situational awareness in emergencies

74

Hurricane Ivan ten years on
Jeremy Collymore traces the path of the hurricane that devastated much of the Caribbean ten years ago, looking at what lessons have been learnt

76

Regulars
Events

80

Calendar dates

83

Looking back

84

EU ECHO

85

Frontline

86

Civil-military interaction p60

Migrant rescue p86

Crisis Response Journal 10:3 | April 2015
Planning for the breach

“You are going to be hacked: Have a plan,” said Josef Demarest, of the FBI. You should also test and exercise that plan. Regina Phelps discusses how to do this

Several years ago they were rare—a big news story simply because they were new. Now, cyber attacks are so common it almost seems like we’re in a world where there is a breach a day. The only thing that separates one from another is how much bigger or deeper the latest one is.

In addition to all of the cyber security protection measures you are taking (hardware, software, procedures, training), you should perform a cyber security exercise to ensure that your management team and business units are as prepared as possible.

Cyber-fear

Your participants could include all or part of: Incident (crisis) management; crisis communications; business units; and information technology and security.

This article will focus on exercising the first three groups, by approaching this scenario from the impact on the organisation, the effects of the incident, and the development of a comprehensive response.

So, what type of exercise works best? In my experience, cyber exercises perform most effectively in one of three formats, whether advanced table-top, functional or full-scale.

These three types of exercises use a simulation. In a table-top exercise, the simulation team plays in person; for the others, the team delivers injects and interacts with exercise players by phone. What is indisputable is that the complexity of this topic requires a simulation team to pull it off; the exercise players need someone to speak to in order to fully understand the problems and issues they are facing.

Our firm designs over 100 exercises every year, and we thought we had seen it all. I was, at first, quite surprised at how this topic affected people. One word sums it up: Fear. Fear of delving into unknown territory, fear of not knowing what will happen next, fear that someone else is in control of what you thought was yours (your data). Some are afraid they will be blamed for the problem (or for not stopping it), even though it is hard to tell where it came from or where it is going, hard to wrap your mind around its full effects, and hard to comprehend its significant reputational and brand impacts.

When designing a cyber exercise with one client’s design team, we found that many of the team members in IT became silent when we asked: “What would take down your systems?” or: “What are your IT weaknesses?” Some were afraid they would be reprimanded for ‘telling secrets’ or they would be blamed for something. We discovered we have to reassure them, and reinforce that everything is said in confidence.

Develop a narrative for your exercise by a deliberate ‘peeling of the onion’ through a series of escalating issues that slowly let the story unfold. First of all, establish that the company could experience a cyber attack. Next, discuss with the team how the attack could be introduced into the system. Phishing, spear phishing, an infected flash drive and watering hole attacks are just some of the possibilities.

But also brainstorm the type of malware that could have been used. For example, the code could have gone undetected for an extended period of time but is not dormant. In other words, the malware might allow undetected data exfiltration or it might allow the attacker to quietly distribute malware through the target’s network prior to launching the attack (this fits the attack profile for many of the most serious breaches that have occurred recently). You should also explore what types of applications or databases could be breached, and the effects if this were to happen.

Go slowly and get buy-in and commitment to each issue. People are likely to be very nervous, so stop periodically to make sure everyone is still breathing!

Keep this in mind about the narrative for your exercise: Determining the exact cause, who did it, and the overall impact is not important. In real life, these questions take days, weeks, or months to fully uncover. Your design job is to make sure that the narrative is feasible and could happen.

If this exercise involves your Incident Management Team (IMT) you might also need to include a coincidental physical impact to engage your entire team, otherwise groups like facilities, security, or business units won’t have much to do. There are lots of simple possibilities to consider.

◆ Protracted power outage;
◆ Construction accident in the immediate area;
◆ Loss of heat (steam) in winter;
◆ Fire in a critical location of the building; and
◆ Infrastructure failure, such as a water pipe break.

Having one of these physical effects occur will make sure that everyone is playing.

Of course, you could always conduct the exercise and only do a partial activation of the IMT, engaging only those who would be affected by a cyber attack.

If you combine a physical outage with the cybersecurity attack, the exercise flow will...
I was, at first, quite surprised at how this topic affected people. One word sums it up: fear.

To reiterate: the exercise designer does not need to know how the security penetration occurred and it will not become known to the exercise players during the exercise. It does matter whether it was owing to a watering hole, malware introduced by thumb drive, software flaw, etc. It just needs to be possible. In our experience, after a good discussion of potential issues, most IT professionals say that a breach is possible 99.99 per cent of the time.

Remember, in this exercise we are focused on effect. Ideally, our perpetrator would have the ability to do any (or all) of the following actions:

- Retrieve information the perpetrator would otherwise not be able to access;
- Make changes to the data (may be for the perpetrator’s benefit, benefit to others, or just to thumb his nose at you);
- Embarrass the company by disclosing private information, shed doubt on the validity of the company information, or put the company on the defensive;
- Disrupt normal business operations; and
- Damage the company’s reputation.

The chances of a breach happening to you are extremely high. It is always better to have some idea of the issues and your response to them, and to identify what you can do now to be more prepared. It is likely to be a matter of when, not if.

**Author**

Regina Phelps is an expert in emergency management and contingency planning, and founder of Emergency Management and Safety Solutions. She is the author of Emergency Management Exercises: From Response to Recovery – Everything you need to know to design a great exercise; just released by Chandi Media.