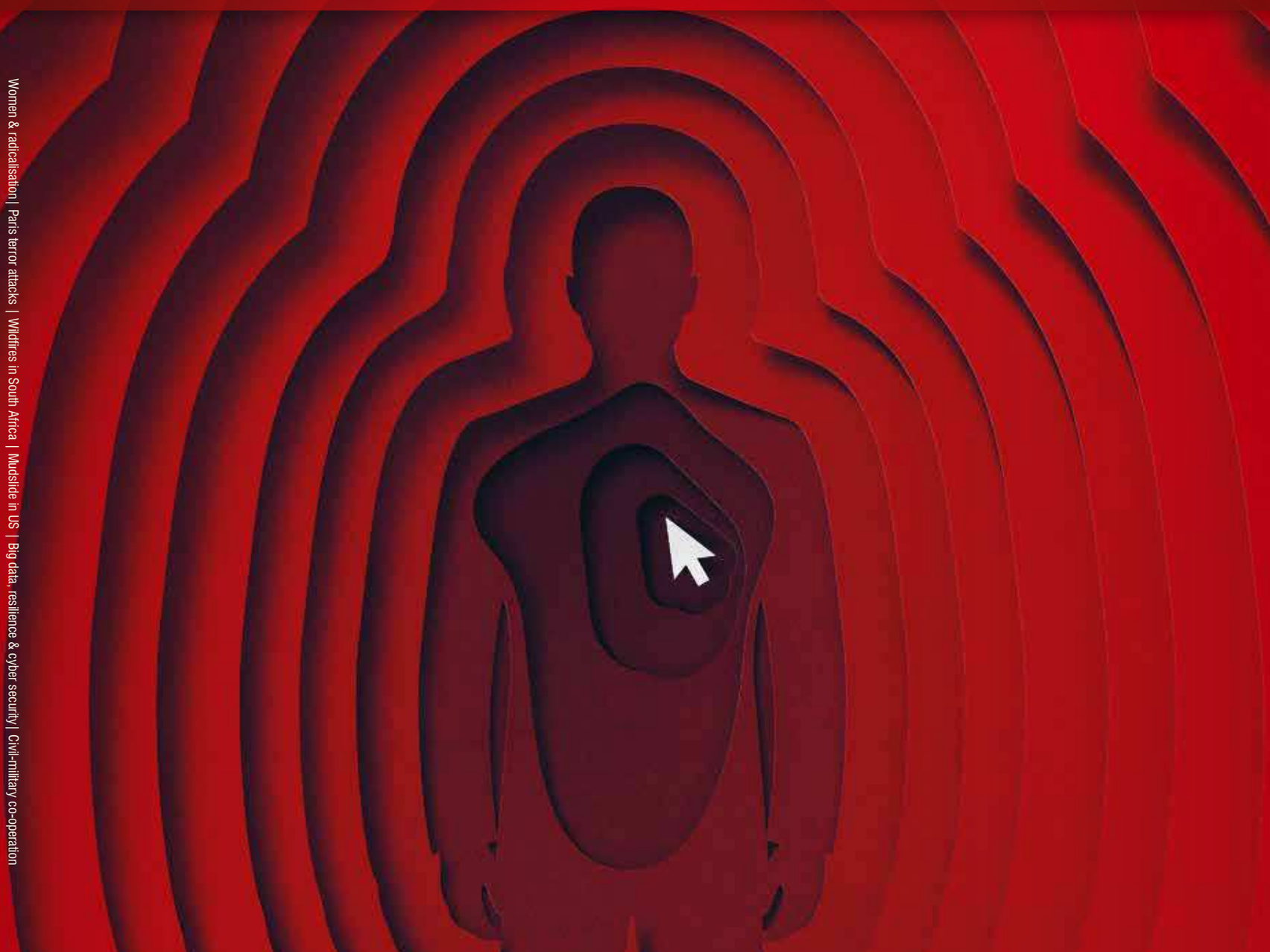
CRISIS RESPONSE

VOL:10 | ISSUE:3 | APRIL 2015

WWW.CRISIS-RESPONSE.COM

JOURNAL

PROTECTION | PREVENTION | PREPAREDNESS | RESPONSE | RESILIENCE | RECOVERY



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

Women & radicalisation | Paris terror attacks | Wildfires in South Africa | Mudslide in US | Big data, resilience & cyber security | Civil-military co-operation

CRISIS RESPONSE VOL:10 | ISSUE:3 | APRIL 2015

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

Design and Production
Tim Baggaley
www.graphicviolence.co.uk

Subscriptions and administration
Emma Wayt
emma.wayt@crisis-response.com

Director
Colin Simpson
colin.simpson@crisis-response.com

Director
Peter Stephenson
peter.stephenson@crisis-response.com

Subscriptions
Crisis Response Journal is published quarterly; it is available by subscription in hard copy, digital format and online. Association discounts, institutional and multiple rates are available; visit our website or contact us for more details
Tel: +44 (0) 208 1661690
subs@fire.org.uk

Back issues
Existing subscribers: £25 (US$45; €36) per hard copy issue (free-of-charge with online access)
Non subscribers: £40 (US$72; €58) per issue
Tel: +44 (0) 208 1661690
backissues@fire.org.uk

Published by FireNet International Ltd
POB 6269, Thatcham, RG19 9JX
United Kingdom
Tel: +44 (0) 208 1661690
mail@fire.org.uk
www.crisis-response.com
www.fire.org.uk

Printed in England by Buxton Press
ISSN 1745-8633

Resources, links, pictures, videos and much more are available for subscribers in our digital and online editions
www.crisis-response.com
join the *CRJ* LinkedIn group
follow us on twitter @editorialcrj

contents

South Africa wildfires p24

Craig McIver | NSRI

Cyber threats: protection advice p44

Eiko Ojala

Cover story: *Big data and disaster response – its potential and its pitfalls, p36*

Main image: Eiko Ojala

In Depth

Regulars

Civil-military interaction p60

shutterstock

Migrant rescue p86

www.moas.eu

comment

At the WCDRR in Sendai, Japan, this March (p4), it was striking how – in the space of around a decade – the holistic nature of disaster risk reduction has been so widely embraced. The breadth of organisations involved has grown dramatically, as has the diversity of the NGOs and sectors represented. Health, finance and economics, science and technology, education, heritage, food security – as well as the private sector, businesses, communities and many more – are now all actively engaged.

The theme of partnerships and involvement, both in response and preparedness, runs through this issue. In the face of today's risks and threats, no sector, discipline or individual should be ignored, or choose to be excluded.

Agreed, this can sometimes make for slightly uncomfortable bedfellows, as is evident from our civil-military feature. The humanitarian and military sectors have increasingly been sharing the same operational space in large-scale crises and this can be an uneasy relationship. Each must work out how to co-operate and fulfill its own mission or mandate without endorsing or jeopardising the safety of the other, or blurring the delineations between military and humanitarian action.

Our cyber security feature also highlights evolving partnerships, especially those between government and private sector entities that might be targets. On p39 Andy Marshall questions what parameters should be set for the plethora of responding organisations during a cyber attack that affects a community or region. The authors on p50 call for co-operation to be enshrined on an international scale. And on p52 Todd Rosenblum spans both features, describing the dynamic between the military and state emergency responders, then making the case for bringing the private sector into a new 'war cabinet' to ensure the US can respond to a massive cyber breach in real time.

The multiplicity of actors involved in disaster reduction, security, response or resilience can be daunting. But all have the same aim: a safer, more secure, sustainable world for communities and businesses, and an efficient, humane and compassionate response for people affected by disasters when they occur. It is therefore vital to eliminate both isolation and duplication of effort.

Emily Hough

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.

The design team must outline the IT failures in detail, noting the date and time of each mini-meltdown. The timeline may look something like Table 1 (days are counting back from the start of the scenario)

Go slowly and get buy-in and commitment to each issue. People are likely 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.

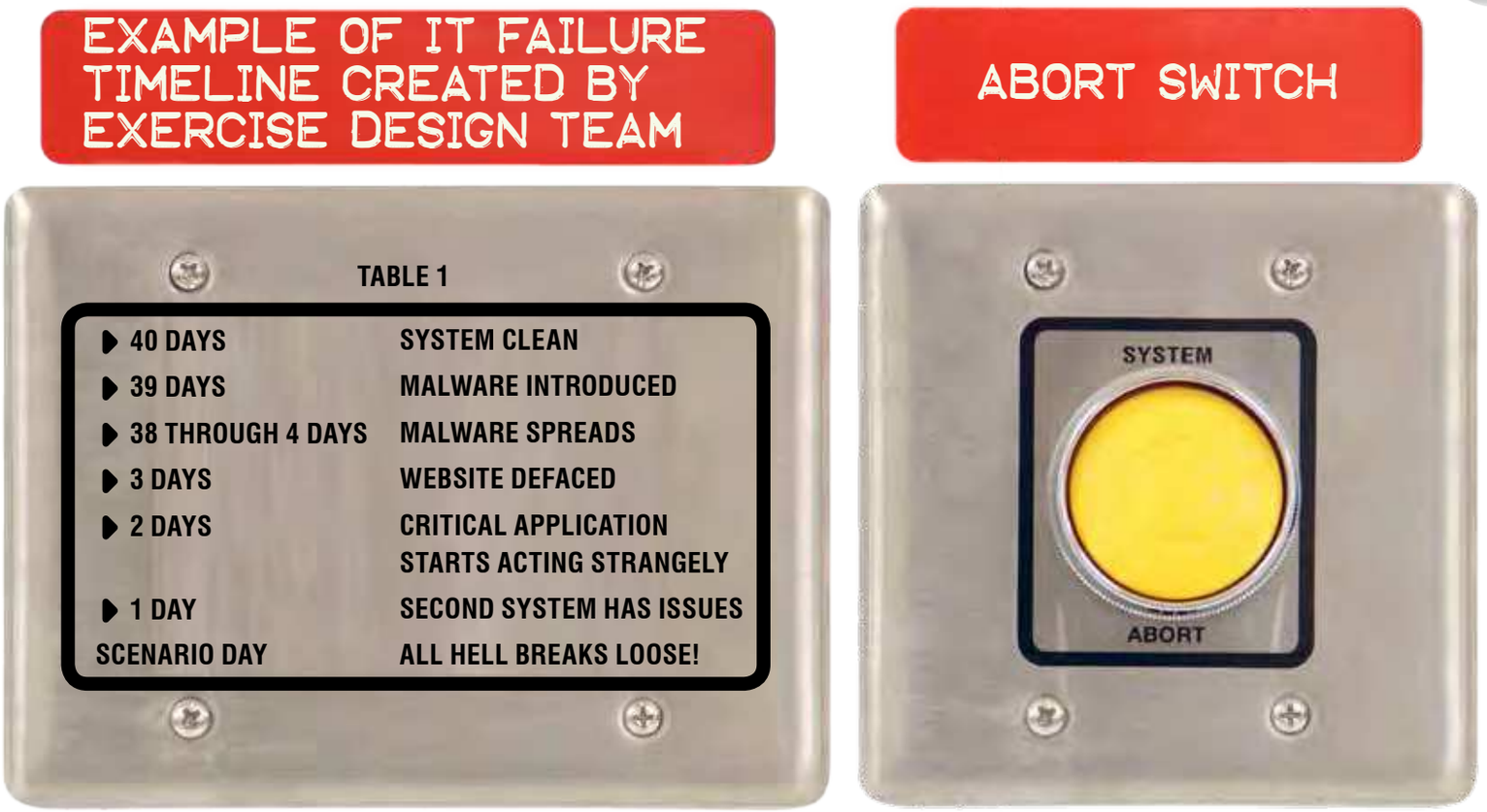
If this exercise involves your Incident Management Team (IMT) you might also need to include a coincidental physical impact to engage your entire team, otherwise groups like facilities, security, or business units won't have much to do. There are lots of simple possibilities to consider.

- 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



have two tracks: the cyber attack, and the physical event. Here are some considerations:

- Information security/cyber attack;
- Begin with a series of simple issues that unfold over a few days;
- Duplicate files;
- Defaced website;
- Strange customer data issues;
- Incorrect instructions; and
- Replicated databases.

Any one of these things, or even two or three, isn't necessarily a big deal, but over a few days, everything begins to pile up.

On the scenario day, the physical event occurs, which causes the activation of the IMT and plan. If you do this, consider whether you should include the incident assessment team and process, and an incident action planning process.

For this exercise to really push the IMT, crisis communications, and the business units, you need to make sure that the event becomes public. We like to produce either a video or audio message from the perpetrator (similar to videos by Anonymous) where the perpetrator is shown in disguise with an altered voice. He tells the company what he's done and what he's planning to do, which is usually to expose information from within your systems.

In your exercise, releasing the video through a social media inject helps to ignite the media fire (this is what the hackers did in the now-infamous Sony breach).

Making the incident public creates a public reputational/brand issue. It will activate crisis communications, engage the company's executives and create anxiety among employees. It will also engage and activate all key stakeholders.

One critical deliverable in the design process is a detailed technology timeline showing when the penetration occurred, where it went, what it did, when it switched on and what happened next. This is used to build the injects, validate the order of the injects, and allows the simulation team to make sure it is on top of the story and the issues. In complicated exercises, it may help to have a small team of IT professionals to develop this timeline.

> I was, at first, quite surprised at how this topic affected people. One word sums it up: fear

The design team must outline the IT failures in detail, noting the date and time of each mini-meltdown. The timeline may look something like Table 1. 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. CR

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*