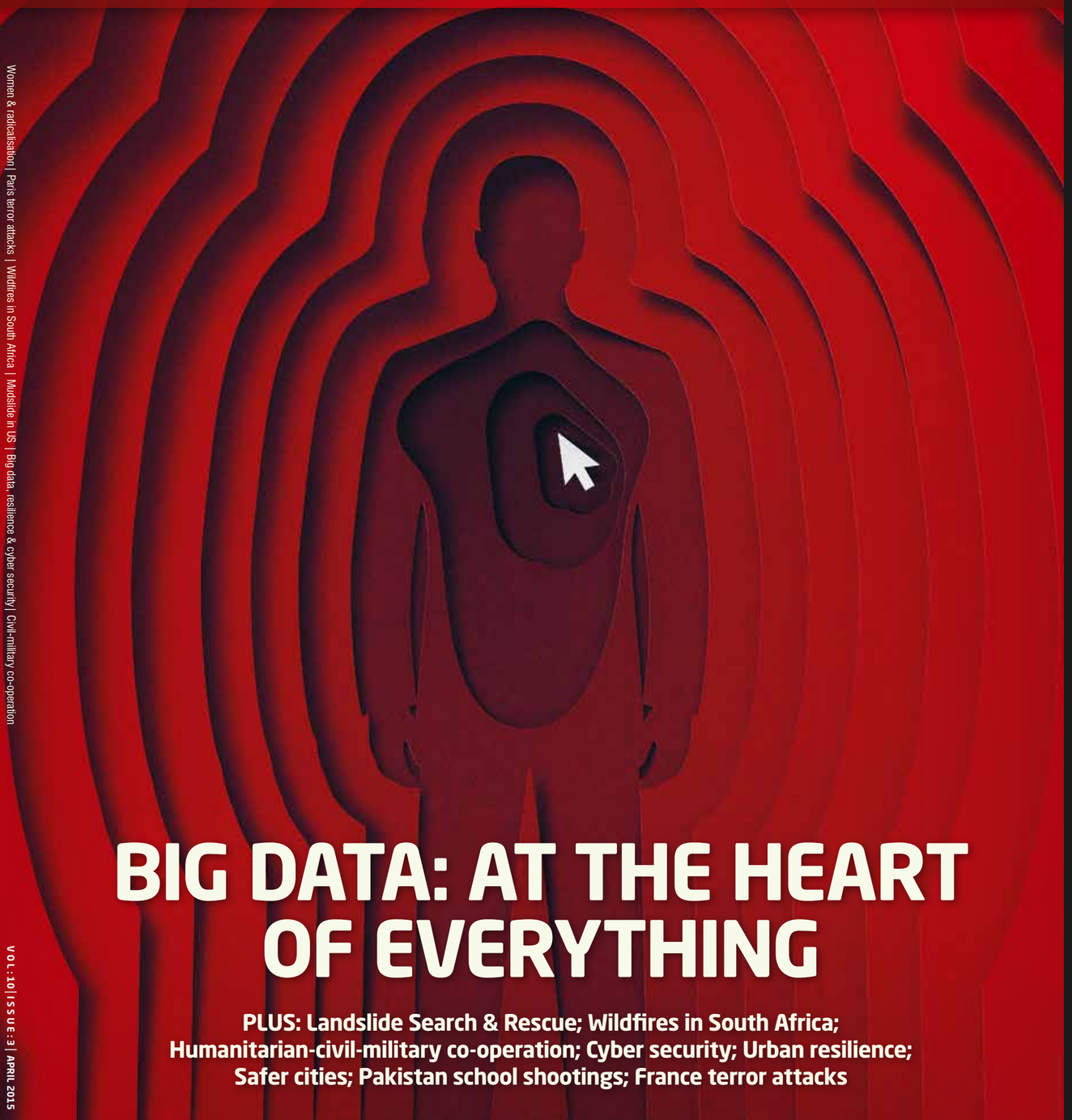
CRISIS RESPONSE

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

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

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

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

Main image: Eiko Ojala

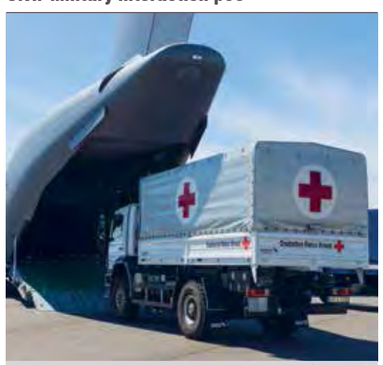
South Africa wildfires p24

Craig McIver | NSRI

Cyber threats: protection advice p44

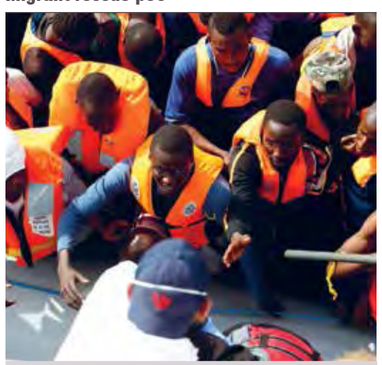
Eiko Ojala

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

Big data alone will not solve your cyber security problems

Today's cyber security threats are dynamic and asymmetric. Organisations need to change their approach to tackle these new threats effectively, says **Chris Morgan**

Companies, governments and NGOs alike need to understand and defend themselves against advanced persistent threats. Cyber attacks are in the headlines nearly every day, and virtually every enterprise has been breached. In the early days of 2015, major breaches against Anthem, Morgan Stanley and the US Central Command's Twitter account have all stolen headlines.

The impact of breaches is tremendous. According to the *Mandiant M-Trends Report*, it takes an average organisation 229 days, or more than seven months, to just detect a data breach. There's a 22 per cent chance that today's data breaches will compromise 10,000 or more records, according to the Ponemon Institute's *2014 Cost of Data Breach Study*. Furthermore, the average cost of a data breach for Fortune 1000 companies has risen 15 per cent over last year to $3.5 (€3.15) million according to the same study. For organisations that store personal health information, partner breaches compromising client information could result in regulatory fines.

Response organisations and Fortune 1000 companies alike all face a similar big data problem in this era of increasing vulnerabilities where attacks are increasingly dynamic and asymmetric in nature. They are happening as constant wave while organisations are becoming more vulnerable through Bring Your Own Device (BYOD) programmes, increasing use of cloud storage, and the Internet of Things. Information security professionals need to optimise their resources to meet the rising cyber security challenges they face.

Critical vulnerabilities can often come from within an organisation: think about the perimeter, but don't forget potential insider vulnerabilities

Igor Stevanovich | Shutterstock

Today, many organisations are looking towards big data and an elaborate network of disparate security systems to thwart these types of attacks. Current network security solutions collect huge amounts of data. In fact, standard security information and event management (SIEM) products collect so much data that companies struggle to operate them. According to the *2013 SIEM Survey* from EiQ Networks, 52 per cent of all companies require two or more full-time analysts to manage their unwieldy SIEM deployments.

This does not account for the additional monetary and personnel resources needed to analyse the extensive amount of data many organisations collect from external threat intelligence feeds, such as FireEye's DTI, Symantec DeepInsights, and iSight Partners.

The problem, according to Mark Nicolett, a managing VP at Gartner, is not that organisations do not have enough security data. "We are not suffering from a lack of data," Nicolett told *Dark Reading*. "We are suffering from a lack of intelligence in analysing it." In other words, collecting more data will be of no help if you cannot find the story within the data.

January 2015: Major breach index — **Table 1**

Total Number of Breaches	8
Total Number of US Gov. Agency Breaches	0
Total Number of Corporate Breaches	8
Potential Number of People Impacted (estimate)	25,985,000
Potential Total Cost of Records Breached (estimate)*	$5,041,090,000

*estimate based on the results from the Ponemon Institute's Cost of a Data Breach (average of $194/record)

But by taking these disparate sets of data out of their resident silos, analysing it and visualising it, organisations can create true business intelligence to find and take action on the small data that counts and ultimately improve their security posture.

So, where are your defences vulnerable? Detecting opportunities requires intelligence tools that can pull security information from seemingly disparate pieces of data. For example, your perimeter tools might monitor frequent SEP alerts from one system, indicating an intrusion attempt. If that point-of-entry is unpatched, threat intelligence would make the connection and alert you to the vulnerability. If it is an access point to critical data that is both unpatched and under assault, threat intelligence would alert you to make it a high-security priority.

Although it is important to defend your network perimeter, it is equally important to consider the human element. Outdated security software was partially to blame for the Home Depot breach in the US, which compromised as many as 56 million customer credit cards. However, Home Depot also employed a senior architect for IT security, Ricky Joe Mitchell, who was sentenced to four years in prison for sabotaging his former employer's security infrastructure.

Users are a critical vulnerability in most organisational defences, particularly in organisations that do not implement granular, role-based access privileges. Think about the perimeter, but do not forget potential insider vulnerabilities.

The current security paradigm is based on a big data approach – an immense amount of data is collected and stored from various sources – log data, external threat intelligence feeds, and open source intelligence (OSINT) data. However, all of this data lives in separate silos. There is no way, and certainly not an efficient way, for even the best cyber analysts to bring this information together to find correlations, relevance or to take action on that data.

An advanced data analytics platform can ferret out the relevant, small data to conquer the big data problem. An effective threat analytics platform can ingest external threat intelligence information and enterprise security data to map known, and potentially previously mitigated, attacks, along with current security data to detect possible attacks already underway. Spikes in visits to and from disreputable IP addresses, domains, URLs, and even specific devices are of utmost importance, as are any compromised endpoint devices calling out to unknown devices and sending sensitive data from your network.

Bringing all of that big data together into one central place in a logical way, and automating previously manually intensive or impractical critical security tasks, allows organisations to increase productivity and reduce the resources required to understand current threats, bolster defences and detect threats. Analysing and representing the full spectrum of internal and external, structured, semi-structured and unstructured data together, visually, allows organisations to find the small data that is meaningful and actionable. Only then can IT professionals effectively deploy limited resources and establish effective protocols for thwarting and addressing breaches.

When you understand the current threats and vulnerabilities faced by your organisation, you can effectively deploy defensive resources to protect the most valuable and / or the most vulnerable assets. In some cases, it might be against systems being disabled using distributed denial of service (DDoS) attacks. In many cases, cyber attacks target proprietary or customer information. Some intrusions leave a backdoor that becomes a foothold for future attacks.

Attack vectors

To find potential attack vectors, an advanced threat analytics approach should examine current CVEs and determine which ones could be used to attack your assets. Trending CVEs allow analysts to provide risk assessment and prioritise patching within the enterprise. Other relevant data include similar advanced persistent threats and zero-day attacks within your industry or sector and reviewing current malware trends and proof of concept exploits, will keep you one step ahead of your attackers. Further, consider third parties that have access to your network (the 2013 Target breach happened after attackers executed a phishing attack on one of Target's third-party HVAC providers, obtaining access to a payment system that Target used to close out vendor work orders. Once they accessed the server that ran the application, they were able to find their way into Target's POS systems). Link charts show associations between exploited internal machines and their external counterparts.

Big data alone is not enough to defend against the ever changing and ever-increasing spectre of cyber threats. By rethinking the way security and threat intelligence data is collected, analysed and reported, security stakeholders can visualise the full threat landscape. This will enable them to find the small data that really matters, allowing them to respond to threats and develop anticipatory security strategies. CRJ

Author

Chris Morgan, *President of IKANOW, has 11 years of experience in project management, systems engineering design, software engineering design and development. In addition, he has extensive experience in operationalising technology solutions into robust and practical products (www.ikanow.com)*