

# CRISIS RESPONSE

VOL:19 | ISSUE:1 | MARCH 2024

WWW.CRISIS-RESPONSE.COM

JOURNAL

Protection Prevention Preparedness Response Resilience Recovery



**SAVIOURS IN CRISIS:**  
BUILDING UP OR BURNING OUT?

Brain Drain & Crisis Managers | Public Warning  
Systems | Middle East Conflict & Ecocide |  
War and Mental Health | Cyber Warfare

**Publishing Editor**

Luavut Zahid  
luavut@crisis-response.com

**Editor Emeritus**

Emily Hough  
emily@crisis-response.com

**Design & Production**

Rizwan Ahmad  
creativesdesign360@gmail.com

**News and Blog research**

Lina Kolesnikova

**Subscriptions**

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

Published by Crisis Reporting Limited,  
71-75 Shelton Street Covent Garden  
London WC2H 9JQ UK  
© Crisis Reporting Limited 2024. Articles published may not be reproduced in any form without prior written permission.  
Printed in England, UK  
ISSN 1745-8633

 [www.crisis-response.com](http://www.crisis-response.com)  
 follow our *CRJ* company page on LinkedIn  
 follow us on X @CRJ\_reports  
 follow us on fb.com/CrisisResponseJournal  
 follow us on @crisisresponsejournal



# contents

## News & Comment

**News** ..... 4  
**Who's truth is it anyway?** ..... 8  
Matt Minshall emphasises the importance of seeking truth for civilised society

**Universities' reputational crisis** .....12  
In the face of a problem, do we listen to crisis managers or lawyers, asks Tony Jaques

## Book Review

**The Lucifer effect** .....16  
Matt Minshall takes a look at Roger Warren's book, *Terrorist movements and the recruitment of Arab foreign fighters*

## Crisis loop

**Measuring risk and resilience** .....18  
Lyndon Bird dissects DRI International's annual trends and predictions report

**No superheroes** ..... 22  
We have failed at planning for professionals in the crisis management industry, says Beverley Griffiths

**Adapting amid change** .....24  
Business environments are dominated by permacrisis, which demands an equilibrium between stability and adaptability, according to Colm Gayton and Elaine Patrao

**Personal crises & managers**..... 27  
The greatest crisis facing resilience professionals is being asked to do more with less and less, says Jeannie Barr

**Manufactured identity & emergency management** .....28  
Is there truly an identity crisis in emergency management, asks Cody Santiago

## Identity crisis p28



Nuvolanevicata | Adobe Stock

**Budget in crisis**..... 30  
Pavel Kiparisov investigates the increased financial uncertainty of public institutions and private companies.

**Mayors as guardian angels**.....34  
Public leaders' role in providing psychosocial care often receives little attention, says Wouter Jong

**Creating a dynamic company** .....38  
In times of crisis, intangible elements matter more than financial balance sheets, say Mostafa Sayyadi & Michael J Provitera

## Security

**Exploring the 'Twilight Zone'** ..... 40  
Novel or combinations of previously insufficiently-analysed crises keep popping up, write Lina Kolesnikova and Michael Kolatchev

**Terror & the Olympics**.....44  
Major sports events are hugely attractive playgrounds for terrorist groups, according to Stefano Betti

**War & ecocide** .....46  
The Russia-Ukraine war and the Israel-Palestine conflict have worsened environmental crises, says Gilles Paché

## Digital attacks & conflict

**Blended threats** .....50  
In a rapidly evolving security landscape, traditional siloed approaches are inadequate, according to Andy Blackwell and John Wood

**Critical infrastructure**..... 52  
Catherine Piana explores the 'Cyber-Physical Security and Critical Infrastructure' report

## War & ecocide p46



Pexels

## comment

**O**verworked, burned out and underpaid, crisis managers are running out of paths to move forwards. Some are leaving their public sector jobs for 'greener' pastures, not out of ambition, but more out of necessity. It takes insurmountable talent to extinguish a burning house when one is doing so from a sinking ship; I'm not quite sure how fair it is for us to expect practitioners to continue doing so.



CRJ's community has informed the pages of this edition in more ways than one. On p22, Beverley Griffiths talks about how crisis managers are failing owing to a lack of planning on how they can find more stability in their careers and, ergo, their lives. Similarly, Jeannie Barr breaks down all the different ways in which the pressure on crisis managers has never been higher, while simultaneously, the resources they have available to them have never been fewer.

This issue has also examines conflict. On p46, Gilles Pache points out that while we focus on immediate humanitarian crises, there is a longer-term bomb waiting for us in the form of environmental decay caused by weapons of war. Stefano Betti dissects terrorism concerns for the upcoming Olympics in France, and Andy Blackwell and John Wood write about how we're increasingly facing blended physical and digital threats and how our defences must be blended too (p50). Nicolò Broglia explores methods for building resilience against digital threats.

It is somewhat poetic that we are also introducing a new section called 'Next Gen' within an edition focused on so many things that are going wrong. Through it, we will explore conceptual solutions with the potential for significant impact. For instance, on p74, we take a look at Gracie Broom and Magdelana Garibaldi's 3D housing concept, which aims to provide immediate and affordable housing for victims of domestic violence.

Where there is darkness, there is light indeed. We just need to acknowledge that there may be a few light bulbs missing.

Cover story: *Saviours in crisis*  
Cover image: Robin Heighway-Bury | Ikon Images

### Cyber resilience & trial by fire .....54

Nicolò Broglia explores methods of building digital resilience

### Redaction tech in surveillance .....58

There is a need to preserve privacy through video data redaction, writes Simon Randall

### Disinformation & resilience..... 60

Crisis managers are not immune to the stresses and turbulence of such emergency situations, says James Lodge

## Response systems

### Emergency operations centres and airport crisis management.....64

Rania Khbais concludes her two-part series...

### School emergencies .....68

Andrew Jaspers analyses recent school emergencies, lessons learned, and best practices

### From failure to triumph .....70

Andre Pugas examines the evolution of vehicle rescue in the Military Fire Department of Santa Catarina

### A tale of Bergen and London..... 72

How do responders make operational decisions and manage their tasks during extended crises? Ilan Kelman, Jarle Eid, and Gianluca Pescaroli take a look

## Next gen

### 3D printed affordable housing..... 74

Gracie Broom and Magdelana Garibaldi describe how trauma-informed design and innovation in construction methods helped to design crisis housing in a tight budget

## Surveillance p58



Freepik

### Designing for disaster .....78

Tori Simpson's work in the Philippines uses design thinking and interdisciplinary research with local partners to create a novel educational tool for disaster preparedness

## Public safety

### Karachi's missing warnings .....82

The urban flooding situation repeats itself with no resolution in sight. Would early warning systems help? Bisma Arif Warraich takes a look

### Recent advances and ongoing challenges for public warnings .....86

Early warning systems are disaster and crisis response functions common to nearly all types of hazards and threats, note Georgios Marios Karagiannis, Gianluca Pescaroli and Sarah Dryhurst investigate further

### Potable water in disaster relief .....88

Robert Kelly highlights the challenges of importing water and emphasises the benefits of providing water locally

### Mental health & conflict ..... 90

Violent attacks in the Middle East had a profound effect on civilians in both the Israeli and Palestinian populations. Marion Leboyer explores a tool for mental health

### Disability & emergency communications.....92

Amy Leete says there is a real need to push for inclusive emergency communications

## Plus

### Events ..... 96

### Frontline ..... 98

EENA 112 Day report

## Affordable housing p74



Gracie Broom

# Blended threats: Synchronising cyber and physical defences

In a rapidly evolving security landscape, traditional siloed approaches are inadequate. Embracing an interconnected, proactive security culture is key, write **Andy Blackwell** and **John Wood**

**I**n today's world of rapid technology advancement, the range of cyber threats has grown enormously beyond our original client base, the aviation sector. Industries such as banking, healthcare, energy, and transportation are now also facing sophisticated and frequent cyberattacks. This pattern shows the pressing need for sturdy cybersecurity measures in all industries, not aviation alone. This article investigates the precise cybersecurity challenges organisations across different sectors are up against, as well as practical strategies they can deploy to safeguard themselves against constantly evolving threats. The key takeaway is that companies across all industries must prioritise building robust cyber defences. With attackers showing no signs of letting up, proactively strengthening cybersecurity must be a priority for every business.

The cybersecurity landscape is an expanding battleground. Advances in technology have massively increased the connectedness of devices and systems. While digital capabilities provide efficiencies, the scale of cyber threats has also grown. These threats now reach all corners of digital services, from personal data theft to attacks on key infrastructure. The attack area goes beyond technology services to the whole operational fabric.

Industries face more hybrid incidents hitting both digital and physical dimensions. For instance, hacking into systems to cause real-world disruptions. These multi-level attacks need a unified response, merging digital and physical security, which few organisations currently have.

## Shake well before use

The UK's Government Communications Headquarters (GCHQ) recently warned that new artificial intelligence (AI) tools will increase cyberattacks globally by making hacking easier for less skilled actors. This will likely drive more ransomware attacks where criminals encrypt systems to demand payment. GCHQ says the effect will be uneven – opportunistic hackers using AI for phishing stand to benefit the most. More advanced state-backed groups are best placed to weaponise AI in sophisticated cyber operations against networks and critical infrastructure. Intelligence agencies see security risks from algorithms that can generate human-like interactions, which businesses widely use in services. Authorities report early signs of hackers utilising these AI capabilities.

An example in the aviation industry is the growing menace of GPS spoofing. It is predicted that the aviation

industry will press regulators for urgent action to help tackle it amid a surge in such activity, which can send commercial airliners off-course. The European Union Aviation Safety Agency (EASA) and the International Air Transport Association (IATA) recently announced the conclusions of a workshop jointly hosted at EASA's headquarters to combat incidents of spoofing and jamming. The workshop's high-level conclusion was that interference with satellite-based services which provide information on the precise position of an aircraft can pose significant challenges to aviation safety. Mitigating these risks requires short-, medium- and long-term measures, beginning with the sharing of incident information and remedies.

But who will tackle the hybrid risks? Cybersecurity and physical security are usually treated as distinct disciplines with separate strategies and teams. Yet, the growing synergy of digital and physical worlds necessitates an interconnected approach to risk management to combat threats which span both domains. Siloed security functions may miss signals or handle incidents poorly owing to limited visibility.

Organisations increasingly will require a unified approach to security defence. Cyber and physical teams must co-ordinate efforts for complete coverage of potential vulnerabilities. Joint planning, shared monitoring, and cross-trained responses are vital to spotting emerging hazards and containing impacts. Though challenging, security convergence remains essential in building hardy, comprehensive protection.

This is not to say there must be a single set of common security tools and terminology. Each team has its own methods, tools and terminology aligned to industry standards. For example, it would be futile to expect cybersecurity teams to use physical security terminology. Instead, an overarching security management system will enable each specialism to report upwards and collaborate in a uniform way without compromising the efficiency and effectiveness of their own operations.

Further, within this overarching security management system, organisations must recognise the need to move to a risk-based model. Meeting physical and cybersecurity security rules helps but doesn't fully protect organisations. Since regulations often trail innovation and new attacks, they create a backward-looking, 'catch up' mindset. For robust defence, to prevent innovative attacks the first time

they are attempted, the rules may not give the necessary protection: companies need to supplement compliance with proactive efforts that get ahead of emerging dangers.

Equally important is building an organisational culture at all levels focused on keeping the people and organisation safe at all levels. This responsibility does not solely lie with the dedicated security teams. A truly robust cybersecurity approach requires company-wide co-ordination. Silos that inhibit co-operation must be dismantled to enable open flows of data and knowledge. When all departments view security as a collective obligation, organisations can spot and address threats faster. By emphasising shared vigilance, they bridge divides, align efforts, and integrate safeguards.

Truly collaborative cultures and methods support proactive defence: unity of purpose throughout makes organisations more adept at identifying and resolving security risks. Everyone benefits when contribution to physical and cyber security is seen as a universal responsibility.

Security does not stop at the front door of the organisation. Prudent security in a networked economy requires disciplined practices with cross-organisation plans for threat assessment, risk management and incident response that are aligned with service providers and other suppliers. With each additional supplier link, new security gaps can emerge. Protecting complex business webs thus becomes vital yet challenging. Diligently vetting service providers is crucial, as are ongoing checks and clarity on shared accountability. Strict assessment of subcontractors via audits and certifications is needed to reduce third-party risk.

All these issues in today's fast-changing security risk environment demand flexible security governance so protections can evolve as threats and technologies do. Static, outdated structures struggle with digital age speed and complexity. Agile models that structurally integrate across operations can rapidly adopt new safeguards without sacrificing business needs. The overarching security framework allows companies to identify and implement new threat controls across silos while ensuring alignment with organisational goals. The result is a resilient foundation for operating at pace: the ability to confidently innovate and exploit new opportunities even as the risk landscape shifts, knowing security policies and practices can be quickly adapted for emerging challenges.

This discussion of methods, organisation and governance should not distract from the critical importance of people. A strong hybrid security approach depends on building talent depth. Adversaries continually evolve tactics; sustained excellence relies on cultivating skilled teams who can outpace emerging threats. This requires staff equipped with leading-edge understanding, backed by advanced AI systems for reinforcement.

In combination, skilled experts and smart systems enable elevated readiness and rapid, precise actions. By creating an environment for security pros to continuously expand competencies while leveraging technology's foresight and precision, organisations can stay ahead of cyber foes.

The discussion of the importance of people is a reminder that the insider threat must be recognised as the silent menace within. Employees or partners, whether



Rawpixel | Freepik

through intentional actions, outside pressure, or honest mistakes, sometimes misuse their expertise and privileges in ways that harm organisations. This danger grows as digital and physical operations interconnect. Companies need to stay alert on two fronts: hardening systems against outside parties while also maintaining oversight of people's activities.

What does all this mean for the overloaded, embattled security managers? The convergence of digital and physical domains expands risks, necessitating integrated protections. All industries must reassess existing practices as networked threats rise. While current measures are a good foundation, continuous adaptation to emerging dangers and technologies is imperative. As cyber and physical worlds collide, threats multiply. An organisation's best defence is an equally collaborative one – security policies, protocols and perspectives that dismantle silos and co-ordinate action across all levels to anticipate risks, block attacks, address incidents and enable continuity. In the face of intensifying threats, accepting security's interconnected nature is the surest path to readiness. **CRJ**

## Authors



ANDY BLACKWELL is the former Head of Security and Resilience with Virgin Atlantic and is now an independent security and resilience consultant in the UK. He is a member of CRJ's Advisory Panel



JOHN WOOD is a Security Management Systems (SeMS) consultant, previously responsible at the UK CAA for security strategy and SeMS, and now specialises in SeMS projects and the development of governance and security management practices in the UK

# 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](http://www.crisis-response.com)

# CRISIS RESPONSE

JOURNAL

PROTECTION | PREVENTION | PREPAREDNESS | RESPONSE | RESILIENCE | RECOVERY



## SUBSCRIBE NOW

visit [www.crisis-response.com](http://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 | DIGITAL