Unseen risk:

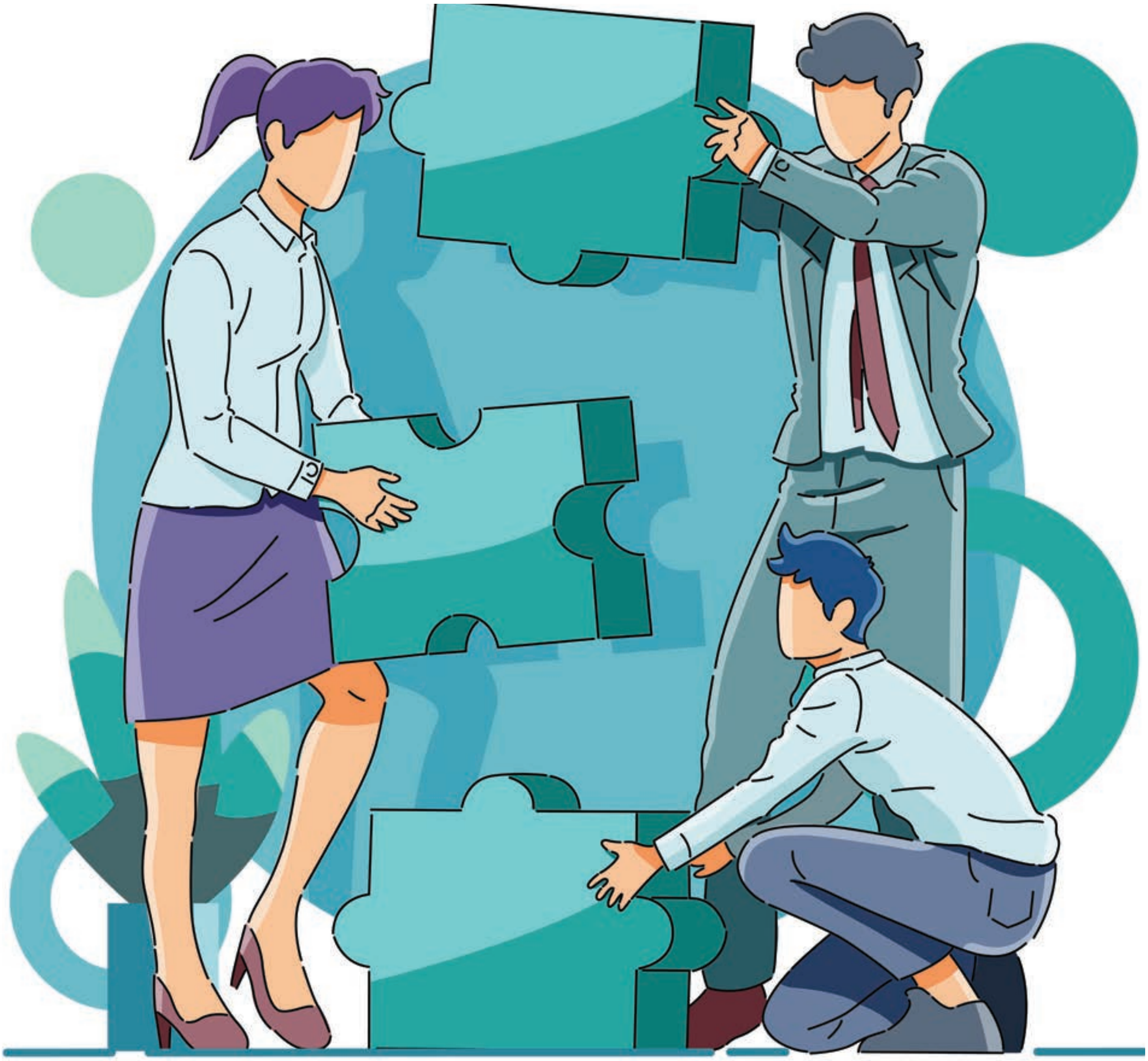
Why security starts with culture, not technology

Security frameworks, both in the tangible and intangible sense, are embedded within a complex system that makes up the fabric of contemporary living, writes **Matthew Porcelli**

Healthcare facilities, supply chains, critical infrastructures, and corporate campuses and their global locations, to name a few, all rely upon the convergence of physical security countermeasures to detect, deter, and delay risk before it evolves into serious incidents or crises. However, even if each individual and department within these complex systems operated smoothly at all times and without errors, which is not empirically feasible, there would still be vulnerabilities that, if not addressed sooner rather than later, could fester, amplify, or even lead to unfavourable outcomes, leaving the asset(s) in jeopardy.

Many organisations have a diverse range of departments. These departments work towards the common goal of ensuring the survival of the organisations or entities, whether that be through operations, sales, compliance, legal matters, and so on. With the inclusion of contractors and subcontractors, which constitute a significant portion of a brand's employment culture, this goal may extend to numerous sub-objectives for the contractors (such as contract security providers and their clients/companies). Owing to the many moving parts and the people in charge of them, there must always be oversight and maintenance regarding the vulnerabilities that may exist among the interconnected components.

This, however, is not always easy because a safety and security culture or crisis avoidance is often approached reactively rather than proactively. Furthermore, there are theories and academic concepts that delve into the importance of recurrent training and awareness, which fuels a complex system or organisation's thinking to better mitigate vulnerabilities and return to normal operations throughout the crisis process. High Reliability Theory or High Reliable Organisations (HROs) seek to: "Explain why some large organisations manage to achieve high levels of performance in the area of safety; redundancy in both human and material resources; the



Vectorkarma | Freepik

Major Erik L J L De Soir *Associate Professiate Professor in Psychotraumatology & Crisis Psychology, Royal Higher Institute of Defence, Belgium*

Brian Dillon *MSc BSc (Hons), expert in counter-terrorism operational response and contingency planning, UK*

Professor Lucy Easthope *is the Deputy Director of Research, Lincoln Law School, University of Lincoln, UK*

Paolo Garonna *Professor of Political Economy, LUISS Guido Carli University of Rome, Italy*

Roger Gomm *QPM, is an advisor, trainer, consultant in crisis and emergency management*

Beverley Griffiths *Senior Lecturer in Emergency Planning, University of Wolverhampton, UK*

Lord Toby Harris *Chair of the National Preparedness Commission, UK*

Dr Jennifer Hesterman *USAF (Ret), VP Watermark Risk Management, adviser Homeland Security Training Institute, USA*

Alice Hill *Senior Fellow for Climate Change Policy at the Council on Foreign Relations, USA*

Brig Gen D Alois A Hirschmugl *Humanitarian Affairs Advisor to Chief of Defence Staff, Austria*

Arn Howitt *MA, PhD, former Executive Director, Ash Center for Democratic Governance & Innovation, John F Kennedy School of Government, Harvard, USA*

Lucian Hudson *Board Chair, Communications Director, former UK Government Chief Spokesperson on climate change*

Haseeb MD Irfanullah *Independent Consultant on Environment, Climate Change & Research Systems, Bangladesh*

Christine Jessup *is a professional educator of more than 35 years, based in Australia*

Ørjan N Karlsson *Specialist Director & research fellow, Nord University, Norway* development of a high reliability culture, notably by means of training; and the comprehension of complex technologies by means of the learning process." (Lagadec 1997). In a perfect world, highly reliable organisations are desirable but not always achievable.

The more complex the system, the greater the potential difficulties in instilling a prominent safety and risk mitigation culture. Security, risk, and other departments tasked with the protection of the tangible and intangible assets of an organisation are more apt to embrace a security-minded culture and remain vigilant for red flags that might cause harm to the organisation and its employees; however, this may not always be a universally shared concept within the organisation's culture.

The most precarious position for an organisation or its leadership is to attempt to learn during an ongoing serious incident or crisis. Chief security officers (CSOs), chief risk officers (CROs), other C-suite executives, members of the business continuity task force, and the frontline security department are all pivotal in ensuring the organisation's safety, security, and survival. Even if these leaders are thoroughly familiar with the crisis response plans for natural or man-made disasters, any lack of synchronisation or familiarity with these plans among other key executives – such as the chief operating officer (COO) or chief information officer (CIO) – can result in significant losses of time, resources, property, and even lives. As Comfort, Sungu, et al (2001) emphasise in their article, *Complex Systems in Crisis: Anticipation and Resilience in Dynamic Environments*: "The critical difference lies in identifying the potential chain of assistance prior to mobilisation for a given event, and building the information infrastructure to support mobilisation, should the need occur."

By establishing a robust security culture and exercising vigilance, organisations can implement resilience strategies that not only benefit themselves, but also assist surrounding organisations and communities in transitioning from crisis to recovery.

Regardless of the size of the organisation, vulnerabilities in the security framework will inevitably exist; conducting vulnerability assessments with the idea that the issues stem from outside aggressors alone is not astute. An organisation does not need to be an electrical substation or a nuclear power plant to activate a sense of security in its thinking. Moreover, vulnerability assessments can be made little by little rather than being thrust into one in the aftermath of serious incidents or a crisis. Furthermore, patchwork mentalities to correct vulnerabilities to save money (such as purchasing inadequate physical security cameras, not fully staffing a security department, and so on) just widen the likelihood of failure of the duty of care of the organisation and its employees. No matter what the premise is, communicating proactively generates and creates a prepared culture. An organisation's departments cannot accomplish anything without effective communication.

Looking ahead

An organisation also needs proactive leadership, and a team leader to initiate, carry out, and maintain vulnerability assessments. Finally, and most importantly, the leader needs to know how to delegate. The more in-house contractors and subcontractors you have associated with a complex organisation (or any size organisation), the more there must be solidification in the hierarchy for clear and concise reporting and communication. For instance, if an organisation's CSO leads its security efforts, a recurring form of communication with the CIO and the management of the contract security department is imperative.

Leadership, regardless of capacity, assumes the uphill battle of navigating the chaos created by a crisis. The key is that not every climb to recovery needs to be so steep. Preparation and recurrent drills are important; however, they must not be viewed as inconvenient necessities. These drills should be staggered, unique, and unannounced, while still maintaining a sense of balance. Negative press and public opinion can leave a stain that many – if not all – entities involved in a crisis will have to contend with; the difference lies in the magnitude of that stain. The public is easily swayed in the wrong direction, and once something is released – whether to the public or within the

Vectorkarma | Freepik

organisation – even briefly before being retracted, it can tarnish reputations and delay both response and recovery efforts. The better prepared leaders are to handle the media and the pessimism that often accompanies crises, the more likely they are to treat the experience as a difficult but valuable lesson rather than a harsh realisation that leaves them asking: "How could it have gone this wrong?"

Vulnerabilities exist in organisations and systems, regardless of their complexity. The key is for security and risk departments to identify and address these weaknesses proactively before they become opportunities for aggressors to carry out nefarious acts or before the aftermath of a natural hazard manifestation becomes so severe that it hinders recovery efforts. Even when the resources to implement appropriate security countermeasures may be limited, adopting a security-conscious mindset – one that encourages identifying vulnerabilities or simply speaking up when something seems off – is an essential first step.

References

- *Comfort LK, Sungu Y, Johnson D and Dunn M (December 2002):* Complex Systems in Crisis: Anticipation and Resilience in Dynamic Environments;
- *Lagadec, P (1997):* Learning Process for Crisis Management in Complex Organisations, Blackwell Publishers Ltd.

Author

MATTHEW PORCELLI *MSc, CPP, CPOI, F.ISRM, FSyI is a safety and security manager based in the US. Porcelli is the North America Hub Chair of the Institute of Strategic Risk Management (ISRM). He is a member of* CRJ*'s Advisory Panel*