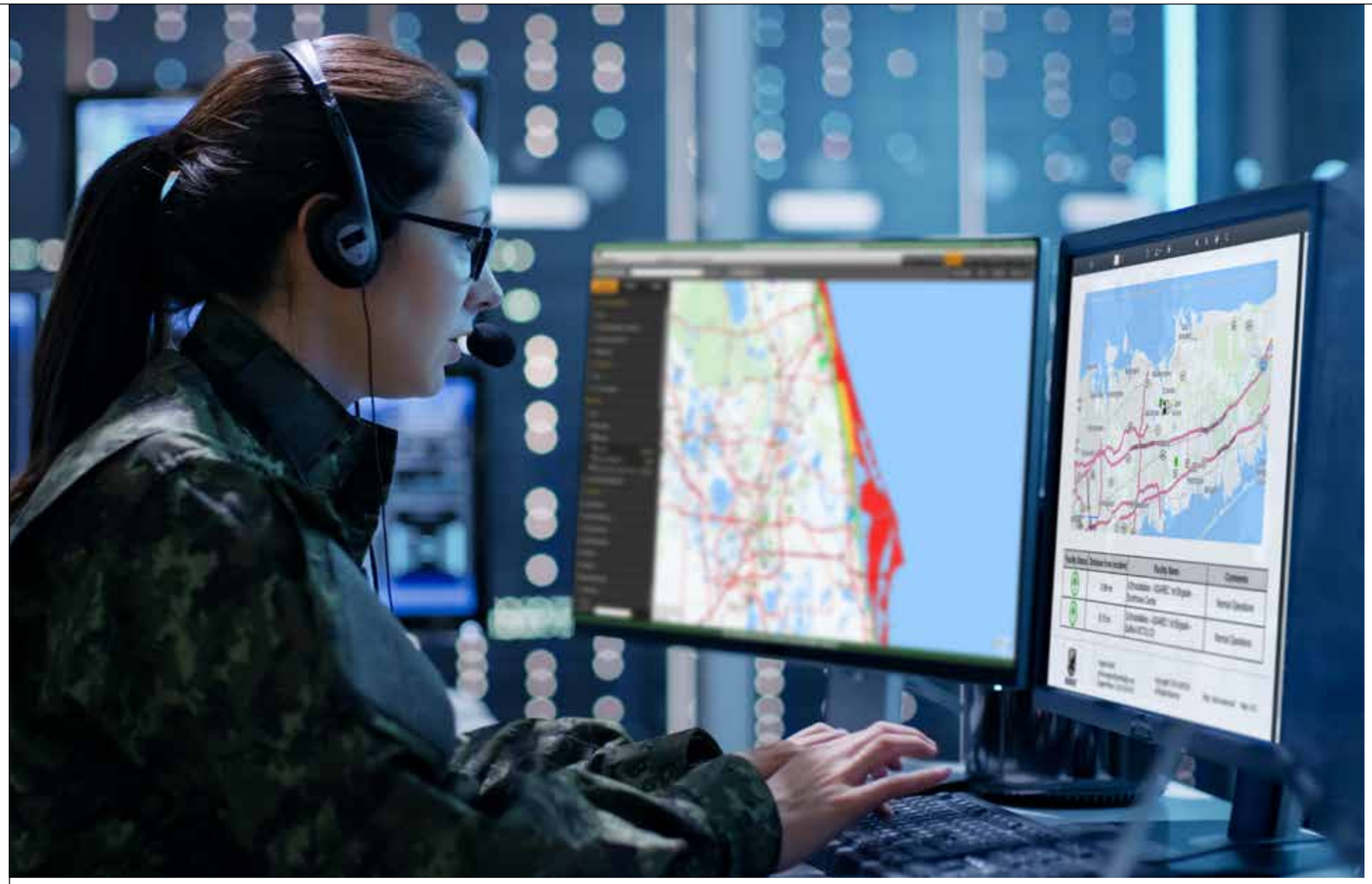

2023: LESSONS LEARNED

Eric Boger *considers the key trends in critical event management over the last year*

As we look back on 2023, it's vital to reflect on what a transformative year it was in the field of critical event management. Throughout the year, we witnessed escalating geopolitical tensions, a huge surge in security threats encompassing both physical and cyber domains, and growing concerns over the intensifying impacts of climate change-induced severe weather events. Simultaneously, the realm of global risk intelligence, early warning systems, and the broader scope of duty of care obligations continue to evolve.

Looking to the year ahead, it becomes increasingly evident that comprehending the profound shifts and advancements characterising this domain is of paramount importance. What becomes clear is that these shifts necessitate a heightened level of preparedness and proactive engagement to navigate the multifaceted challenges and opportunities on the horizon. With a focus on informed adaptability and agility, we must not only acknowledge the past but also embrace the future, forging a path forward that ensures the safety, resilience and prosperity of all those under our duty of care.

International cooperation and data sharing strengthens early warning systems, helping communities and organisations better prepare for crises.

Several key developments have marked significant milestones in the integration of physical and cyber security in the past year. In the United States, the Department of Homeland Security introduced a comprehensive cyber security framework, placing a strong emphasis on merging the worlds of physical and digital security. This strategic move aimed to safeguard both online and offline assets effectively. Research carried out in the UK among chief security officers from 30 countries, found that 90 percent agreed that AI is set to have the biggest impact on physical security operations in the next five years. The report from G4S also revealed that 33 percent of CSOs in the UK would be investing in AI and machine learning to improve physical and cyber security operations. In some areas in the private sector, this is already being done with prominent enterprises escalating their investments in AI-powered surveillance systems. In 2023 these cutting-edge systems not only excelled at detecting physical breaches, but also exhibited the ability to identify cyber threats, offering a holistic and all-encompassing security solution.

So, what are the lessons we have learned when it comes to the exploration of cyber security vulnerabilities? In 2023, a surge in cyber-attacks exposed vulnerabilities across various sectors. Notable data breaches and ransomware incidents underscored the importance of proactive and adaptable cyber security measures.

And looking at critical infrastructure under siege, there was a substantial uptick in attacks on critical infrastructure, including power grids, water supply systems and transportation networks. These incidents highlighted the vulnerability of such systems to cyber threats, necessitating urgent security enhancements.

There is a vital role for AI and machine learning in security where they can assume a central role in threat detection and response. In 2023, cyber security solutions increasingly harnessed these technologies to analyse extensive data, detect anomalies and automate incident response, leading to quicker and more precise threat identification and mitigation.

The other area in which there has been elevated emphasis is on supply chain security. Recognising the potential risks posed by supply chain vulnerabilities, organisations have elevated their focus on supply chain security as a top priority.

The year was marked by significant geopolitical tensions, open hostilities and a strategic surprise with the 7 October Hamas attack on targets in Israel. A global environment with this level of dynamism underscores the critical role of risk intelligence in supporting the decision-making and sense-making of global enterprises.

Despite concerns over inflation and economic downturn, many multinational companies continued to invest in the size and capability of their risk intelligence teams to include the leveraging of generative AI, exploitation of new sources and adding new partners into their tech stack.

The lessons we have learned in this regard are that real-time risk intelligence is more essential than ever while the world experiences surges in geopolitical tensions and uncertainty, which is particularly marked in regions such as Israel, the Middle East, Eastern Europe and the South China Sea.

Severe weather events have been experienced across the globe, disrupting supply chains and exacerbating geopolitical tensions. This is the impact of climate change, and it presents a growing and significant risk factor.

One of the positives has been in the area of advanced analytics. Risk intelligence firms developed more sophisticated analytical tools, enabling better predictions of geopolitical events and their impact on businesses and governments.

Persistent climate change trends, with their escalating impact on severe weather events, have pushed climate change mitigation to the forefront of critical event management, underscoring the paramount importance of disaster preparedness.

In the public sector, the National Oceanic and Atmospheric Administration (NOAA) harnessed advanced climate modelling and early warning systems to issue remarkably accurate forecasts for extreme weather events. These forecasts facilitated efficient evacuation plans and substantially reduced the loss

GOVERNMENTS WILL INTRODUCE STRICTER DATA PROTECTION AND CYBER SECURITY REGULATIONS

of life during hurricanes and floods that occurred in 2023. In the corporate sphere, retail giants responded with strategic investments in resilient infrastructure and diversification of supply chains to adapt to climate change impacts. For example, a prominent retail corporation integrated climate data into its risk assessment, prompting timely relocations of distribution centres away from flood-prone areas.

The entire world is learning lessons, often the hard way, from severe weather as a result of the climate crisis. However, in 2023 governments employed AI to improve their response to natural disasters. For example, machine learning algorithms were used to predict flood patterns and allocate resources effectively. In addition, severe weather led to heightened investments in infrastructure resilience. A notable example was the reconstruction of coastal areas in a number of countries with more resilient designs, better prepared to withstand storms.

A notable shift took place in the insurance sector where companies adapted to the changing landscape by developing innovative policies that considered climate change risks, ensuring better coverage for property and businesses in high-risk areas.

Travel risk management took on new dimensions in 2023. TRM evolved to encompass broader safety and well-being concerns, emphasising the duty of care towards all employees regardless of their work location.

Diplomatic missions took proactive steps to enhance support for expatriates and embassy personnel abroad, introducing real-time tracking systems to monitor their movements. This measure was particularly crucial in response to civil unrest or natural disasters, enabling swift responses to ensure the safety of citizens. Likewise, corporations embraced a comprehensive approach to employee well-being during travel, leveraging advanced data analytics to monitor their workforce's health and safety. This extended not only to health guidelines amid the ongoing pandemic, but also included safety precautions and the provision of psychological support.

As a result of lessons learned, changes have been made in the health and safety sector with travel risk management incorporating and amplifying the

significance of health concerns, such as pandemics, as a key factor in risk assessments.

Advanced data analytics and monitoring tools have helped organisations make real-time decisions based on up-to-the-minute information. And the concept of 'duty of care' gained importance as organisations were increasingly held accountable for their they' safety while travelling or working from a non-traditional location.

33 PERCENT OF CSOS IN THE UK WILL BE INVESTING IN AI AND MACHINE LEARNING FOR SECURITY

In 2023, early warning systems, whether designed for natural disasters, cyber security threats, or geopolitical events, witnessed notable enhancements and expansions. The UK is a prime example, with the roll-out of the population alerting service in April, which can now be used to reach people quickly in an emergency or where there is a risk to life.

In 2023, these systems became increasingly interconnected, bolstering their efficiency and adaptability to address intricate, hybrid threats. Nations took a more collaborative approach to early warning systems, forging unified responses to combat hybrid threats. For instance, a noteworthy collaborative effort involved countering a cyber attack on critical infrastructure by deploying a combination of cyber experts and security forces.

Furthermore, large enterprises harnessed the power of AI-enhanced early warning systems to anticipate and manage cyber attacks and geopolitical crises, especially those with cyber components. This proactive approach aimed to safeguard sensitive data and valuable assets.

What are the lessons learned? Certainly, international cooperation and data sharing strengthens early warning systems, helping communities and organisations better prepare for crises. We also know that AI-driven early warning systems became more accurate, enabling quicker responses to emerging threats. When it comes to hybrid threats, early warning systems can now address these, involving a combination of physical and cyber threats or geopolitical and climate-related risks.

As we step into 2024, there are eight significant trends that will persistently influence critical event management:

Holistic Approach: Organisations and governments will adopt a more holistic approach to critical event management, addressing physical, cyber and environmental risks in an integrated manner.

AI and Automation: The use of AI and automation will continue to expand, enabling more effective threat detection and response in both the physical and cyber domains. Organisations will invest in AI-driven solutions to detect and respond to risks in real-time, improving overall security postures.

Continued Climate Focus: Climate change mitigation and adaptation will remain central in risk assessments and resilience planning.

Ransomware Resilience: Organisations will prioritise ransomware resilience by implementing robust backup and recovery strategies. The focus will shift towards data protection and ensuring business continuity in the face of ransomware attacks.

Supply Chain Security: With the increasing reliance on global supply chains, 2024 will see a greater emphasis on supply chain security. Organisations will use thorough risk assessments and audits to identify and mitigate vulnerabilities within their supply chains.

Resilience as a Priority: Resilience planning will become a primary focus, with increased investments in infrastructure and strategies to mitigate the impacts of climate change and geopolitical tensions.

Regulatory Compliance: Governments and regulatory bodies will introduce stricter data protection and cyber security regulations, emphasising compliance and accountability. Organisations will need to adapt to these evolving legal landscapes.

Enhanced Early Warning Systems: Early warning systems will continue to improve, leveraging cutting-edge technologies and global cooperation to provide more reliable alerts ●

Eric Boger is VP Risk Intelligence at Everbridge

Corporations have embraced a comprehensive approach to employee well-being during travel, leveraging advanced data analytics to monitor their health and safety.