ISARR

KEEP IT SIMPLE RISK, RESILIENCE & SECURITY IN AN UNCERTAIN WORLD

With organisations across the globe busy planning how best to resume business after the COVID-19 lockdown, Andy Blackwell, ISARR's Senior Risk and Security Advisor, provides insights into what businesses can do to keep their people and assets safe, and maintain a high level of resilience despite the uncertain times ahead.

↓

A 'BACK TO BASICS' APPROACH?

Rather than trying to second guess the future, a back to basics approach focusing on what the organisation can do right now to prevent incidents becoming crises, will prevent knee-jerk responses and the inherent risks they bring. Keeping things simple and getting the basics right will also help

organisations stay on track during periods of rapid, and what is likely to be chaotic, periods of change as business resumption commences.

Building a solid 'security and resilience' foundation will make it easier for organisations to adapt and extend their programmes going forward, once they have assurance that their baseline security and resilience is robust. Companies who have implemented a Security Management System (SeMS) such as the UK's CAA CAP1223 model will already have a solid framework to help them manage risk sensibly, and assure their security and resilience performance.

Review Your Risk Assessments

One of the first steps organisations are well advised to take is to review their 'threat landscape', as changes in operating environments, such as staff working from home, may have reduced some threats but increased others. Some of the 'old' threats such as international terrorism haven't gone away, and Islamist terrorist groups see the global chaos from COVID-19 as an opportunity to mobilise and prepare for the future. Their modus operandi has always been to target the path of least resistance, and any weakness, or indeed perceived weaknesses in our security capabilities will be exploited by them. Cyber criminals have intensified their efforts of late, and two of San Francisco Airport's low traffic websites were recently hacked resulting in data being unlawfully obtained.

Once the impacts of the current threat landscape have been established, organisations should review their risk registers to ascertain that the risks, their scores and mitigations remain fit for purposes, reflecting any changes and new risks identified.

IDENTIFYING WARNING SIGNALS

Many businesses have been severely impacted by the COVID-19 lockdown, with some reporting that their business continuity plans were not as robust as they could or perhaps should have been. A review of the learning from the organisation's response to the crises, good and bad, should be a priority task. It is also worth looking externally too for best practices, or issues identified that may help shape your plans going forward.

The words of Sir Winston Churchill *"Never let a good crisis go to waste"* resonate with me at the moment. These are challenging times for us all, without question, but provide so many opportunities to learn and make things better and more resilient for the future. A no-blame frank discussion with all key stakeholders will invariably yield far better results than finger-pointing.

Established academic research suggests that all crises are preceded by warning signals and the ability of organisations to be able to detect and interpret these can often make the difference between managing an incident or trying to survive a crisis.

In the transport sector perhaps the most significant example of missed warning signals was the 9-11 attacks. The Report of the Joint Inquiry Into The Terrorist Attacks of September 11, 2001, by the House Permanent Select Committee on Intelligence and the Senate Select Committee On Intelligence, provides us with some useful insights: firstly that the US Intelligence Community failed to fully capitalise on available and potentially important information and secondly, that from at least 1994,

and continuing into the summer of 2001, the Intelligence Community received information indicating that terrorists were contemplating, among other means of attack, the use of aircraft as weapons. This information did not stimulate any specific Intelligence Community assessment of, or collective U.S. Government reaction to this form of threat.

Another aviation example is the 'Underpants bomber' Umar Farouq Abdulmutallab's attempt to detonate his improvised explosive device on board Northwest flight 253 over Detroit on Christmas Day 2009. Fortunately the device failed to detonate properly and the only injuries were sustained by the perpetrator. Plenty of warning signals were said to have preceded the attack, but weren't assimilated or progressed sufficiently to prevent Abdulmutallab from boarding the aircraft and conducting his attack.

Another example from outside the sector is the 2019 Easter Sunday terrorist attacks in Sri Lanka which killed 300 people and injured 500. Unfortunately warning signs were again ignored and the authorities criticised for failing to share information that could have stopped the attacks from taking place.

The good news is we know there are opportunities to identify potential crises before they actually happen. How good our company radar is at identifying the warning signals, and how good our risk managers are at determining the harm they pose together with the mitigation required, will much dictate the type of outcome we experience.

Missing warning signals, late identification, or misinterpreting them due to other noise or distractions could be catastrophic for the organisation.

COMMUNICATING WARNING SIGNALS

Other challenges are linked to the communication of the warning signals. There needs to be timely identification, collection and sharing across a multidisciplinary team, with the experience to rapidly and accurately assess the direction and action for signals of concern. It is no use warning signals being detected if they are not rapidly communicated to the key decision makers such as a Risk Assessment Group (RAG) and the Board.

The wider the composition of the multidisciplinary team (e.g. the RAG) the richer the risk picture. Gone are the days where the security team had information supremacy, in today's corporate world, other areas of the business are likely to have unique knowledge to help inform the risk picture. The more pieces of the jigsaw we can join up, the closer we will be to seeing the whole picture.

An organisation's poor sensitivity to risk can result in routine incidents or disruptive events becoming crises. Denial is the biggest cause of risk sensitivity, with organisations wrongly believing that the identified risk will not impact them, or that the magnitude is not as severe as it actually is. The term predictable surprise has been used by academics to describe crises resulting from the failure of individuals and organisations to act on what they know.

One key characteristic of highly reliable organisations is their ability to identify, interpret and respond properly to warning signals. A recent example of this is Prague Airport's detection of attempted attacks on its web pages, where their timely identification and mitigating actions thwarted the crime in the early preparatory stages. The airport's proactive approach resulted in them receiving positive media coverage, and their action clearly demonstrates their positive approach to security. It's no surprise that the airport has been actively championing SeMS approaches at their annual SAFSEC conferences.

The ability to rapidly access relevant and reliable information remains central to organisations scanning for warning signals. The ever increasing number of sources available and the proliferation of social media channels, can make this a challenging task.

It is not just about looking for a needle in a haystack, it's trying to ascertain which haystack to look in. Monitoring of social media can give early insights, for example; a sudden increase in social media posts from certain areas may indicate something untoward is going on, Breaking news often first breaks on social media before being rebroadcast via the established media channels (but care needs to be taken to corroborate such information) Social sentiment monitoring can also provide us with useful foresight.

SUMMARY

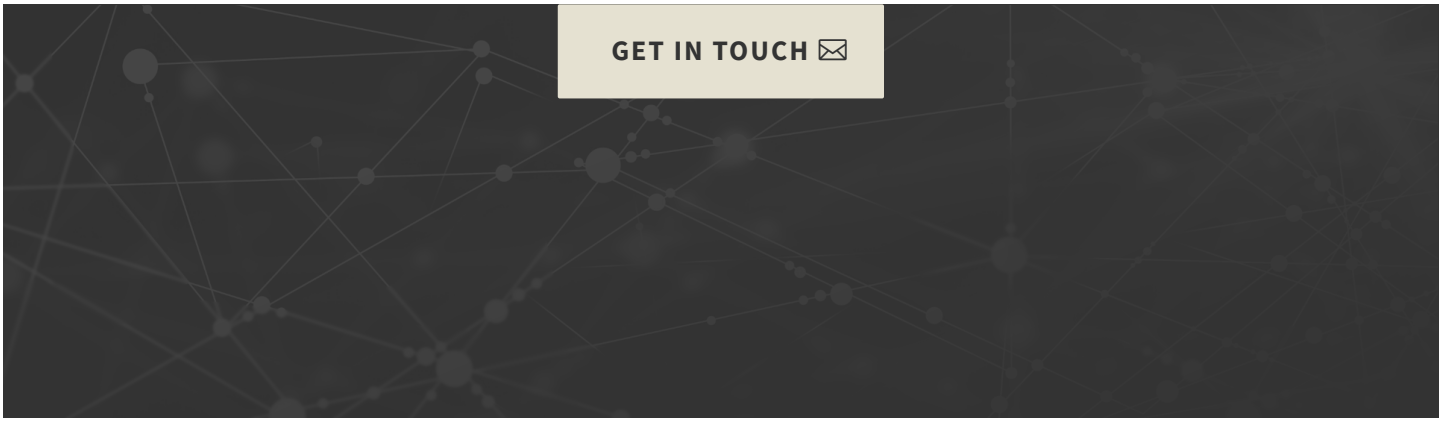
A summary of the key actions organisations are recommended to consider are:

- Understand the current threat landscape and how it impacts your organisation
- Review your risk register and make any necessary adjustments
- Identify and implement lessons identified from the COVID-19 pandemic response
- Assure your security and resilience provision
- Scan for warning signals

This article has outlined key actions organisations can take to protect their people, assets and operations. The guidance is aligned with established Security Management System (SeMS) principles and recommends a keep it simple, back to basics approach, with a constant focus on the detection of, and response to warning signals. Future articles will be focused on how ISARR's range of web based management information and operational tools can help Intelligence, Security and Risk Resilience Leaders.

FURTHER INFORMATION

If you are interested in further information about the system, would like a demo, or even arrange an initial telephone chat, you can get in touch using the "Contact Us" button below



Location

85 Great Portland Street, First Floor, London W1W 7LT

Office Number 0203 4750 753

Subscribe

Subscribe to our newsletter to stay up to date with our most recent articles and updates.

SUBSCRIBE