ISARR

WE’RE ONLY HUMAN: MANAGING SECURITY THREAT AND RISK UNDER PRESSURE

Andy Blackwell, a Senior Risk and Security Advisor with ISARR, examines how organisations have been managing security threats and risks during the COVID-19 pandemic, and identifies several human factors having a direct bearing on security and resilience.

DURING COVID-19

The quote '*Anyone can hold the helm when the sea is calm*', attributed to Publilius Syrus 85-43 BC, tells us that it is easy to lead when things are going well, but a very different story when operating in stormy seas. The same applies to how organisations manage their security threats and risks, the less pressure on the organisation and its people, the easier it is to keep the organisation safe and secure, but during an incident or crisis, where the operating environment becomes fast paced, dynamic and emotionally charged, people become stressed, and the effectiveness of decision making is much more dependent on who is at the helm, their support team and the information, tools and systems available to them. The COVID-19 pandemic has whipped up a dangerous and enduring storm, creating uncertainty and a climate of fear. Holding the helm today and dealing with 21st Century crises is complex and challenging, requiring decisive leadership, diverse thinking, agility, and clarity of communications.

Let us look at how organisations have fared overall since the emergence of COVID-19. They broadly fit into three categories:

> Firstly, those who were completely surprised by the pandemic and as a result were literally 'bowled over' by the event and its aftermath despite this risk type featuring on national risk registers for many years. Risk management and resilience activities in these organisations were weak and immature, and as a result the businesses are unlikely to survive. Let us call this group the **VICTIMS**, although in most cases they have put themselves in this position due to their lack of foresight and planning. Their false assumption that "*this will*

never happen to us" highlights their risk blindness, and in all likelihood their ability to survive any crisis or major incident would have resulted in the same outcome due to their position on the survival chain.

Secondly there were those who were aware of the risk of a pandemic but misjudged the magnitude and longer-term implications for their organisation. Many of the businesses we researched fall into this category and coped due to the strength of their existing risk management and resilience capabilities. Whilst these organisations are likely to survive, it will take them several years to recover their financial position. We will call these the **SURVIVORS** but the nature of 21st Century crises is such that it is not just about surviving, but thriving……. and this leads us on to our final category:

The smallest grouping by far, but the most favourably placed, are the **THRIVERS**, those organisations who fully understood the pandemic risk, had prepared for such an eventuality, recognising and exploiting the opportunities it could bring. These businesses bear all the hallmarks of high reliability organisations. One such international company we spoke to, which has a presence in Asia, identified the warning signals and took robust protective measures at least three weeks before the full extent of the pandemic was widely understood in Europe. This early action afforded maximum protection to their staff and facilitated remote working before government requirements came into effect. A week before the government-imposed lockdown, the company had fully tested remote working for its key workers.

Having established the broad groupings let us now focus on how businesses have been managing their security threats and risks and look at some of the **human factors** coming into play. Threat and risk management is the core of a robust security management system (SeMS) and high reliability organisations are adept at keeping their finger on the pulse, ensuring threats and risks are identified, appropriately managed, and any emerging opportunities exploited swiftly. Organisations who fail or are unable to monitor these ‘vital signs’ place at risk their people, their businesses and in some cases the public at large.

We regularly see claims by organisations that security is their number one priority, most frequently cited after some accident or major security breach or other untoward event. If it was the organisation’s top priority the event is unlikely to have occurred in the first place, or would have been managed more effectively. There is often a mismatch between the resources assigned to this ‘number one’ priority versus other business activities such as sales and marketing. The top priority for most organisations will be profitability, and this is fine provided safety and security are at the forefront of everything the organisation does. So perhaps the number one priority should be ‘Growing a profitable business, safely and securely’, or as some organisations now state ‘Safety and Security are top priorities, subtly different than them being the number one priority, and more authentic.

As we have said before, getting the security and resilience balance right is key, as is being transparent. And on the topic of transparency, the behaviours of some organisations during Covid-19 conflict with their public statements about their commitment to safety and security. Of concern are some who disregarded their existing security and risk management protocols and just did what made sense to them at the time, primarily due to the significant organisational pressure from above to cut costs. Whilst I am all for innovation and diverse thinking, this type of pressured response can be problematic and not only place people at risk but put the organisation in breach of its regulatory obligations. It will also prove challenging for those organisations to justify why they deviated from their tried and tested protocols and procedures, particularly if something untoward occurs due to inadequate security, threat and risk management. Not surprisingly, organisations with mature **Security Management Systems (SeMS)** generally fared better than those without one, as their practices and methodologies were fully understood, extensively used and trusted. They did not need to deviate from what they already had, it was proven, agile and fit for purpose.

The furloughing of specialists also created challenges and on occasions took some incumbents out of their comfort zone due to the limited subject matter knowledge they had, and on occasions their lack of experience. This ‘hidden risk’ could reduce the organisation’s situational awareness and consequently the quality of their threat and risk management activities.

There are also human factors dilemmas for staff who may be at risk of redundancy and are fearful of challenging the decisions of those senior to them, even though they may be uncomfortable with the risk exposure, or carrying out what is asked of them. They may feel that they are under greater scrutiny than normal and be wary about ‘rocking the boat’. The prevailing organisational culture will of course have a significant influence on how the employee will react, together with the individual’s own values and personal culture. From the safety world we know the dangers of failing to challenge, or hesitant challenging due to what is often referred to as dominance dynamics, with research suggesting that up to 20% of all aircraft accidents may be preventable by optimising the monitoring and challenging of Captain errors by the First Officer. Studies by the US National Transportation Safety Board report that more than 30 aircraft crashes have occurred after co-pilots failed to communicate their concerns. Much vigour on the human factors front has been applied, to good effect, in the safety domain, and the same level of vigour needs to be applied to security. Organisations in the ‘thrive category’ understand what drives performance, and recognise human limitations. Their approach to human factors is proactive, as opposed to those who would just react to what would be predictable variables such as staff returning to work after long periods of furlough.

UK Prime Minister Boris Johnson recently made comments advising that although organisations have learned huge lessons about the potential of technology throughout the lockdown, it was no substitute for human interaction and face-to-face conversations. This statement has relevance in the world of threat and risk assessment, with some existing human factors challenges being magnified in the virtual environment. Online meetings tend to feel quite staged and do not really work for brainstorming. It is difficult to pick up on the unsaid word, and participants can easily get distracted and become disengaged. Many of the discussions in the margins of traditional meetings are often the most potent and identify ‘real’ issues. Virtual meetings are largely devoid of this, reducing their effectiveness, and tend to get dominated by the stronger people in the group, whilst the quieter ones who may have crucial information about particular threats and risks can’t break into the discussion, get talked over, or fail to share crucial information due to the belief that others must already be aware of it. One simple solution, relevant to face to face and virtual domains, is to let the leader or most powerful people speak last, so that the views of others can be captured early on in the meeting and their views are not influenced by what their boss may say.

It is certainly not all bad news on the technology front though, with many organisations reporting that productivity of their workforce has been maintained, and in some cases **increased** albeit in a remote environment. Specialist platforms and modules are also helping organisations identify threat warning signals, gather and share information, and display insights in a way that helps the Board and Crisis Commanders make timely and informed judgements about threat and risk.

CONCLUSION

How businesses manage security, threat and risk in ‘stormy seas’ provides a useful insight into management commitment and organisational culture, highlighting the extent to which human factors influence the actions and behaviours of their people. Much vigour on the human factors front has been applied, to good effect, in the safety domain, and the same level of vigour needs to be applied to security and resilience.

Walking the talk (management commitment) is not just for the calm seas, and having the right person at the helm, supported by an experienced, capable and diverse team with ready access to management information and operational tools will help organisations brave the storm and navigate safely to calmer waters.

Whilst it is reassuring that organisations with mature security management systems (SeMS) have fared better than those without such a framework, it is concerning to hear that some businesses disregarded the proven principles and ‘did their own thing’ due to significant pressure from above to cut costs. The need for appropriate oversight has never been greater.

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

GET IN TOUCH ✉

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