Security solutions providers support **the strategic approach to risk and resilience**

Security providers are experienced in dealing with a range of risks so are well placed to advise on how to prepare, what to do when things go wrong and the potential impact and consequences.

Today's rapidly changing political and environmental landscape has created a risk climate that evolves. Everybody has increased connectivity and this reliance on technology increases risks. Threats arise from human and environmental hazards; our clients are now vulnerable to new risks. Understanding these risks and our response is important so we can test and exercise scenarios.

Advising on the risks

The source of the threats can be predicted. Currently, we operate in a COVID-19 backdrop but the recognition that a pandemic can be a threat was known, however, the response was unprepared. The strategic policies of governments will impact our client's strategic goals. Examining the national and local risk registers can provide understanding of the environment clients operate in. As a security provider, we draw upon expertise to determine the impact to the client. Security providers have dealt with and lived through many of the risks so we can provide advice for when things go wrong, what the knock-on effect may be, and direct and indirect consequences.

In particular, Business Continuity Management is an area where a security provider can assist in mitigating risks. Gaining an understanding of what is the most important products and services is key and the associated activities and resources needed to keep our client's strategic goals operating.

Developing the tactical response

Risk reports focus on historic events but predicting the future is where we can help clients. As a security provider, we can provide security responses for our client's strategic goals. Currently, COVID-19 is considered a near miss and whilst we are still in the midst of it, de-briefing the response monthly and understanding our learning objectives provides strong grounding to tackle future threats. Our response and considerations have developed throughout the pandemic, this has been a great source of learning for our team. Many organisations run Gold, Silver, Bronze responses but can senior managers put their hands on their hearts and say they understand what their role is and what a Gold commander is responsible for? Or have they run this in a live scenario? We need to consider a tactical response to threats reported in the National Risk register. We are able to test and exercise the responses to many identified threats, which will ensure continuity of operations, plan for disruption to staff, office space, and supply chains. We can work to provide a business continuity plan to be more than a coffee table document but a live document we all understand.

Improving knowledge and expertise across an organisation

To develop security expertise across an organisation, initially, you have to consider the holy trinity of educational theory domains: cognitive i.e. knowledge connected to the understanding of law, policies, good practice and decision-making processes; the psychomotor domain i.e. the practical application, applying it to a person's physical skills; and most importantly the 'affective' domain i.e. an individual's attitude, their mind-set and motivation.

Once you understand this 'baseline' of your organisation's ability and need, there are key requirements starting with an experienced practitioner(s) who have the range of skills to educate, develop and nurture.

We must factor in COVID-19 due to the impact and restrictions it places upon all of us, but also for how it will positively change the future. We will always have the spectre of the virus looming. Therefore, lessons learned regarding remote delivery, spacing, hygiene, travel etc. will become the new norm and will be part of the infrastructure of training design and delivery.

There must be the vision, investment, support and drive from all aspects of the business management to make this process work. Only then can you construct appropriate methodologies suitable for the range of profiles in the diverse, busy, and geographically challenging locations that all modern security companies now have responsibility for.

Recovering from the pandemic

Companies may now invest in intelligence capabilities to scan longer term threats. This will allow for forward planning to mitigate threats and provide commercial advantage. Provision of experienced individuals who have a capability to manage dynamic threats particularly in relation to business continuity.

The pandemic is likely to stay in various forms, and we must ensure we prepare for foreseeable scenarios:

- A full return to work with minimal restrictions
- A structured return to work with a number of restrictions
- Potential variants of the disease which may require full lockdown.

We must also look at what other threats are present, or which may result from the consequences of this pandemic. Companies now operate differently since the pandemic. Companies may now utilise the same premises more efficiently. Before they may have had 10,000 people working in an office Monday to Friday. They may now have 15,000 working in that office for shorter periods but at different times/days. This provides a balance of benefits of working from home and office life. Consequently, security structures must be flexible and agile. A key area is likely to be smarter solutions around Flexible Access Control.

How the security sector is evolving

The security sector's greatest strength is diversity, both in terms of personnel, and range of experience. Better information sharing is necessary to prevent and detect threats. It can also enhance emergency preparedness and response. This is evident through networks such as the. City Security Council. Many public private partnerships exist in cyber security where the development of cooperation models makes this business as usual.

Models exist for private security to begin to take on functions traditionally carried out by law enforcement, like guarding at government buildings and crime scene management: many low-level investigations not requiring senior oversite or forensic evidence. There needs to be a mindset change that emergency services cannot meet current demands and private security can help fulfil this.

We can detect, protect, prevent and deter crime within a geographic area through visible presence and agreed responses to events. This would allow public services to focus elsewhere and increase safety. Initially, collaboration will create dilemmas, but partnerships already exist, such as private ambulance services. Examining regulatory frameworks would ensure responsibilities are clearly defined and provide understanding of each other's roles. Increasing communication can only negate the scepticism and increase the trust fundamental for mutual respect.

Adrian Moore
Operation Director
Allied Universal

www.aus.uk.com