Addressing your CEO's sleepless nights

What has free thinking and entrepreneurship to do with security?

Plenty if you work in security and risk management for the right company, where it is aligned to a centralised advisory structure.

What has terrorism to do with the corporation? Very little today, unless it causes collateral damage. But in the future, corporations could be culpable for allowing company assets to be used to aid terrorists under new legislation being explored by the government.

There is a failure by some organisations to understand the array of geo-political risks they face. Or, an overreaction to compliance is seen in the three lines of defence model implemented by some financial organisations, with a belief that defence in depth will mitigate most challenges.

But is the point of failure – the human being – still going to defeat this sophistication?

Today's security function is about using a variety of business skills to implement an integrated, flexible, commercially astute global response to the range of risks.

My organisation, SSR Personnel, has recently worked with a group of global corporations to look ahead to 2020 to understand how the corporate security function might expand or downsize.

Working with Chief Security Officers (CSO) and Heads of Security across a range of sectors that included financial services, manufacturing, extractives, pharmaceuticals, defence and global services, we asked twenty-two questions about security governance, structures and reporting lines, the threats, analytical capability and the convergence between cyber and traditional security.

Our research thus far indicates, as you would suspect, there is no absolute model for security governance, but there are some key trends which depend to a certain extent on the nature of the business. In effect, international manufacturing and production businesses with large physical sites key to the supply of their product tend to have a more centralised structure. International service businesses require security services for the people and assets of the corporation in the locations where they are facilitating trade, which could be some of the world's most dangerous regions.

We looked at the corporate security structure reporting line and how many levels that was from the Chief Executive's office. It is evident that the increasing regulatory requirements of the past six years have caused the shift into the Risk function with many companies taking a more holistic view of risk. This strongly features cyber: in particular, cyber dependence versus cyber vulnerability

The Global CSO tends to have a relatively short reporting line – sometimes direct – into the senior echelon (President/Senior Vice President level) of the business coupled with very close relationships with regional security heads. It is this relationship that sets the tone of risk management, be that compliance, regulatory or security.

The Chief Security Officer (CSO) is the business champion who will stop the Executive Board members panicking if caught in a terrorist incident.

The relationships between the CEO and the Global CSO in service businesses tend to be more distant, with sometimes a number of layers of management in between, and in these businesses the relationship with regional heads of security seems more likely to be a dotted line, with a firm line into the regional business head.

In both cases a "design in the centre, deliver in the regions" model for security seems to be emerging. The centre is seen as the provider of enterprise policies and procedures, risk and threat assessments and monitoring. The regional heads deliver operational security except for some very specific skill sets.

With terrorism risks, corporations are often blindsided without policies in place as to the next actions in the event of, say: a shooting in your offices or on your street; an attack on a next door office; the bombing of a facility previously not considered at risk. Terrorism targeting of your facilities could expose a systemic failure and under investment in the security structure of the organisation. The changing risks and threats, including direct action against companies from ISIS or political pressure groups, have shown Government alone can't deal with that, companies will have to become involved.

The risks include the insider threat. Corporations in the past have looked at the disaffected, now we have to consider the radicalised. The vehicle driver in your organisation was once a risk through ill health or bad judgement, or a systems failure that might cause a crash. The radicalised driver now can have a similar impact to a bomb, murdering or maiming many citizens, such we have seen with vehicle projectiles in Nice and Berlin.

What has been common in speaking with our CSOs is that the creditability of the security function is high where the CSO has invested in risk intelligence to remove the flotsam provided by some sources and tailor-make reports that the CEO and Board can access quickly to broaden their understanding in an incident. This generally means the corporate security function includes an analyst capability, outsourced or in-house, that searches all open source intelligence and dissects threats throughout their sphere of operations. Where that is not in place, the consensus is that you need to convince the c-suite to invest in awareness programs within an analytical process to ensure that the emerging threats are identified in a timely way. This is hugely important as it impinges on all our ways of working.

With cyber, the debate is currently focusing on the convergence between IT and physical security and the different mindsets required. Yet all roles can be different. Banks and their customers now lose more money through exterior deception than ATM deception or bank robberies, so who should own the risk? As a Head of Security remarked: "The importance of having the cyber prevention discipline in your cupboard is otherwise you have the safe and the keys – only to find out that someone has taken the secrets."

Further insights from the research programme will be available during 2017.

Peter French
Managing Director. SSR Personnel

www.ssr-personnel.com