The Security Manager of Tomorrow

Who manages security? The response to this question is most likely to be: "The security manager, of course." Maybe this remains the situation in some organisations. However, as Mike Kenny describes, the traditional notion of protection being all about officers, fencing and alarms ' to create a secure, crime-controlled environment' is unlikely to be the most appropriate, holistic or business-orientated management strategy for the modern-day risk professional

Mike Kenny CSyP: Training Manager at ARC Training

For today's security manager, analysis needs to centre on 'what is security and how is it perceived?' Security has various connotations and perceptions, both positive and negative. In the present globalised corporate environment, perception has significant influence. The usual – some might say predictable – application of primarily physical and technical measures restricts mitigation options to the oft-quoted quartet of 'deterrence, detection, delay or response' mechanisms when looking at asset protection.

In the 'shape-shifting' world of the blended threat, such as a combined cyber attack on both physical and logical security systems, the use of the term 'security' may be difficult to fully articulate before a sceptical audience, and particularly so if the approach to providing the organisation's security is silo-based wherein physical asset security has little interaction with those providing logical security elements.

This underlines the dilemma of security terminology. Using 'security' as a term may not be appropriate in certain organisations. Creative enterprises with globalised, de-layered and/or matrix organisational structures and a youthful entrepreneurial demographic may hold negative perceptions of 'security'. The security function may struggle to communicate what 'security' means within an organisation.

In the case where key company assets such as brand, reputation or a proprietary business methodology are intangible, the security manager may be better advised to 'brand' their security approach as 'protection' and avoid the potentially negative perception of the term 'security' altogether.

Fitting in with the strategy

The security manager must assess where they fit into the commercial strategy of their enterprise and the value they bring to the organisation. Security often struggles to shed itself of the ingrained perceptions of being a cost centre rather than a profit centre. Return on investment is key for most business units, and the security manager needs to be able to quantify – or qualify – where they add value.

For Risk UK's readers who are scanning this article beware. Your management may well be contemplating that question right now and asking: "Who should we have managing our security?" Potentially, you may be the problem.

As security – to use a collective noun that encompasses risk, loss and protection *et al* – is a business function, is there a need to employ business people or security people? A long-standing dilemma, and one that's often argued, is that in the traditional sphere of security it's the wisdom of 'hands on' experience that prevails over business knowledge.

However, the old routes to entry – from the police service or the Armed Forces – may be viewed as restrictive in the competencies they purport to bring to the security sector. To add to existing experience, the 'second career' security practitioner has to be able to demonstrate business acumen, develop positive working relationships within the organisation and evidence contribution to the bottom line. These are now prerequisites.

As one academic commentator puts it: "First, the security industry needs to move away from the ex-policeman's (and it's usually men) second career image. The security manager needs to be perceived as a risk professional in their own right" (Borodzicz, 2005).

The security sector has evolved since 2005, but the issues of being perceived as a non-professional industry sector still persist, albeit for a variety of reasons.

Traction being gained through the increasing realisation within the security world that educational, vocational and professional competency is essential if we're to gain the necessary respect within commercial arenas as 'business enablers' is cause for great optimism.

Security or risk?

Let's return to the earlier question: 'What is security?' As highlighted, the term 'security' can be perceived as having negative connotations and perception is everything. The security manager has a number of tools at their disposal to determine how (traditional) security should be deployed. Methodologies have developed over a number of years, usually by sector. For example, the oil and gas industry has the American Petroleum Institute's Security Vulnerability Assessment firmly in place.

With increasing recognition for international standardisation, the recently-published Risk Assessment Standard RA.1-2015 (developed by ASIS International in partnership with the Risk and Insurance Management Society and accredited by the American National Standards Institute) provides a system for demonstrating a sound and consistent methodology towards evaluating risk-based decisions and developing security mitigation strategies.

These methodologies should be used to inform and align thinking on risk, but not be prescriptive or deterministic. If a collaborative risk methodology is used across an organisation then this should enable the security manager to elevate the sphere of influence of the security function and provide a 'step change' towards security as a business enabler. This is the catalyst for the security manager to then adopt or promote the methodology of Enterprise Risk Management.

As mentioned, the security manager needs to be recognised as a risk professional within his or her own enterprise. Therefore, the question as to who manages security becomes subservient to the requirement for quantifying risk across the organisation.

There should be a commonality of purpose and a standard mechanism in order that the enterprise as a whole manages risk. The issue of security, therefore, becomes the implementation of control measures. These are owned by all business functions.

The establishment of an Enterprise Risk Committee or Risk Council ensures that the security function demonstrates its overall effectiveness at executive level. The security manager should be collaborating across the enterprise to challenge and shape perceptions in order that the security function is synonymous with risk management. Ergo, as Borodzicz observed, the security manager becomes the risk professional.

Agile and business-focused

The agile and business-focused security manager must be able to demonstrate understanding of the threats facing the organisation in both the static ('pure') and the business ('dynamic') risk landscape in order to convince the C-Suite that the enterprise security function is a business enabler.

Notwithstanding that managing risk demands we implement security through appropriate controls, the security manager must be aligned to the business strategy by identifying – and operating in concert – with their business unit peers. They must be able to identify the political, economic, market, brand and potential compliance risks. Unchartered territory for a good majority of 'second career' security managers, it must be said.

The kinetic threat posed by the exponential rise in cyber crime looms large as recent events at TalkTalk will testify. This is an environment where the security manager must seek to control the narrative and promote effectiveness. Acknowledging the interdependency of physical and logical security is paramount if we're to understand the threats and provide a cohesive organisational mitigation strategy.

The spectrum of enterprise assets extends beyond the established security manager classifications such as people, property, information, operational continuity and reputation. Brand, environment, communities, supply chain and a host of tangible and intangible assets are now vulnerable across the enterprise portfolio.

The challenge for today's practising security manager is to acknowledge an understanding of the logical vulnerabilities that an enterprise now faces in the flux of a global risk landscape. This demands both a strategic and tactical knowledge of the technologies that secure an organisation's assets.

Collaboration, building key Board-level relationships and contributing to an organisation's business strategy forms the framework for sound risk management that will ultimately inform the risk and security management mitigation process.

Recognising that Enterprise Risk Management and security convergence are now key elements within the risk and security management equation is the important baseline upon which the 21st Century security manager must operate.

In time, the ideal scenario would be to elevate the role from security manager to risk professional and enterprise strategist.

"The security manager should be collaborating across the enterprise to challenge and shape perceptions in order that the security function is synonymous with risk management"