Physical, Electronic and IT Security Convergence for Risk Management and Control

MATTHEW HACKLING

Matthew is an Account Director in Deloitte's Security and Privacy practice. He currently provides IT security testing to ASX companies and government. Matthew was previously employed as a physical and electronic security consultant for an engineering firm. Comments on this article are welcome to mhackling@deloitte.com.au

Matthew Hackling considers progress towards a convergent approach to enterprise security.

The convergence of physical and IT security functions within enterprises is likened to the early days of flight. Visionaries have attempted to take their organisations in this direction and progress has been slow and difficult, but there is no doubt that "convergence" is intuitive and logical.

Deloitte was commissioned by the Alliance for Enterprise Security Risk Management (AESRM) to research and develop a report addressing the value of security as a part of enterprise risk management (ERM) and the benefit of a converged view of security in managing enterprise risk.

ERM is a top-down process that looks across the entire organisation and improves its preparedness to identify and respond to risks that can either positively or negatively affect the organisation. It's probably no surprise to security professionals that the research indicates that executives see security as having a utility value and being a tactical function that is not required or beneficial for higher level business processes or decision making.

Current focus on operational security initiatives from the research shows that the emphasis is on business continuity planning, data security, identity and access management, security training/awareness, infrastructure improvement, application security and centralised security information management respectively.

Organisational initiatives in order of importance were compliance, governance, strategy, reporting and measurement and integration of physical and information security strategies respectively. The top threat-based initiatives in 2007 were directed at the following threats respectively: malicious attacks, employee misconduct, identity theft and account fraud, insider fraud and natural disasters.

The drivers for convergence as identified from those interviewed were aligned with the following:

- Better risk of combined threats
- Increased information sharing
- Better protection of people, intellectual property and assets
- Regulatory compliance
- Cost savings
- Single point of contact
- Better alignment with corporate goals

The most important value propositions for convergence from those interviewed were:

- Enhanced security
- Cost-efficiency
- Enhanced compliance
- Enhanced productivity
- Faster response
- Enhanced incident correlation
- Cleaner audit and compliance
- Accountability across the enterprise
- Sustainable, repeatable and predictable processes
- Strategic growth support
- Better user experience

Obstacles to convergence are:

- Cultural barriers
- Process/change management
- Training/Knowledge gaps
- Lack of direction from C-suite
- Salary issues
- Risk of adverse consequences

Activities required for convergence identified in the research include:

- Leadership alignment
- Communication strategy and execution
- Organisation design, including job and role profiling
- Stakeholder management
- Performance and performance management systems
- Organisation culture assessment
- Learning management systems and programs

A relevant case study is worth referencing. SAP is one of the world's largest software companies with over 38,000 employees. Their problem was that they had no centralised security policy and governing body to the nearly 100 employees for whom security was their main responsibility. Their solution was in 2004 to combine the information security and physical security teams into one global security organisation. The virtual security team is made up of more than 80 security professionals who have the role of security officer in addition to their business line responsibilities. The security officers are governed by a corporate security group of 14 people who provide guidance, training, strategy, requirements and solutions as well as setting the baselines for security. Each of the security officers is responsible for all aspects of physical and IT security within their function and is expected to comply with the guidelines set by the security steering committee. While the security organisation is responsible for providing information regarding security risk, SAP has a separate global risk management group of similar size working only on risk management.

In summary, if you are considering convergence of your security functions, within your organisation, be sure to consider the above drivers, value propositions, obstacles and typical activities in your business case to the C-suite. ■