Assuring management of the effectiveness of security

The need

In this age of uncertainty, dynamic threats and security events will continue to be a way of life for the industry. How an organisation responds to them speaks volumes about their security certainty.

In the past, security has been entrusted to security professionals with little oversight from top management. Corporate governance is coming under growing scrutiny by regulators, pressure groups and the media; and the absence of effective governance exacerbates the weaknesses in traditional security measures, with regulators increasingly taking the view that compliance with regulations is not enough.

Owners and management of the organisation need assurance of the security of their operations in the widest sense, a dynamic and effective approach not simply those aspects required for compliance. The regulations deal with yesterday's known threats; and an inspection is only a snapshot in a particular location at a particular time, a statistically unrepresentative sample that cannot be relied upon as a good yardstick.

The solution – a systems thinking approach to Security Management

A Security Management System (SeMS) delivers corporate assurance. It provides similar management controls to those used in prudent financial management. An effective SeMS identifies and controls risks, and manages budgets and resources. It establishes a reliable governance regime with delegated authorities, escalation of issues to appropriate management levels and easy to assimilate management reporting.

> "A SeMS is an organised, systematic approach to managing security which embeds security management into the day to day activities of an organisation. It provides the necessary organisational structure, accountabilities, policies and procedures to ensure effective oversight. In summary, a SeMS is an assurance system for security."
>
> *UK Civil Aviation Authority*

Pro-active not just reactive

The significant 'target hardening' of the industry has largely resulted from a 'cat and mouse' game with those seeking to cause us harm, versus the protectors. Getting ahead of the game will always be a challenge despite the best efforts of regulators and industry. From what we have seen repeatedly, lack of management insight into security risks is behind the 'rush' to abundance of caution. Their lack of knowledge of their organisation's security performance and resilience results in them doing what they consider to be the lowest risk option. In reality, abundance of caution creates a false sense of security.

The more certainty the organisation has about its security performance and resilience, the more able it is to make informed judgements about threat and risk. In such an organisation, management understands the risks their organisation faces and has confidence in the measures in place to mitigate them. The best of these organisations have also established a no-blame culture which reduces disproportionate responses to threats and other dynamic security events, since executives, managers and staff no longer feel compelled to 'cover their backs' and are comfortable taking a measured response.

Not expensive, not difficult

Despite these attributes, a SeMS is not expensive or difficult. It exploits the security arrangements already in existence, co-ordinating and enhancing them organically rather than buying new tools. Such a home-grown SeMS is so powerful as a weapon against would be attackers precisely because it builds on the existing tried and tested arrangements and develops the staff skills and management capability.

Growing your own SeMS

The SeMS is a development of the existing security processes, people and technology. It is an agile development enabling prototyping and evolutionary changes to be delivered quickly. The focus is on a 'home grown' system, where the security team and the management accountable for security are equipped and guided to develop the existing security measures and governance into a fully effective security management system.

The four stages of SeMS development

The emphasis is on enabling and supporting the client to develop its own SeMS, with periodic injections of guidance, practical help and mentoring. This minimises both the consultancy costs but also the internal resource costs.

Initial Assessment and Scoping

A high level exercise to determine the overall scope of a SeMS appropriate to the organisation's operations.

Requirements Analysis and Business Case

Based on the Initial Assessment, a full requirements analysis and business case can be constructed.

Implementation

If the business case is approved, the SeMS Implementation can be planned and executed

Evolution

A self-sustaining improvement process that makes use of various aspects of the SeMS itself.

Initial Assessment and Scoping

The first step is to answer key questions about the development of a SeMS specifically aligned to the organisation's needs. We conduct a short workshop with the security manager and colleagues. From this we develop a report of our findings, with options and recommendations on how to proceed with a SeMS project.

Requirements Analysis and Business Case

Following discussion of our Assessment report, we guide the analysis of requirements and development of a project proposal and business case in the format used by the organisation for governance of its projects.

Implementation

Following approval of the project proposal and Business Case, we conduct a planning workshop with the client to produce the Implementation Plan. This will determine the Implementation activities, pace and timescale. For many aspects of the SeMS, the client's existing processes and systems will be adopted, and adapted or enhanced where necessary. There are some specific aspects that are usually the least mature and may be better left for the Evolution phase. If required, we can offer methods, templates, training and software solutions as appropriate.

Evolution

Developing the SeMS is an evolutionary process. The Implementation phase is focused on establishing a self-sustaining SeMS that the client can take forward unaided. Once that has been cemented, components integral to the SeMS, such as Continuous Improvement, will drive the evolution forward as an element of SeMS Business-As-Usual. This approach allows the SeMS to complete its Implementation phase – an important milestone – without being delayed by longer term and continuing activities such as cultural evolution, cross-campus awareness education, or software implementation.

Benefits of an effective SeMS

The purpose of the SeMS is to enhance your protection of employees, stakeholders, partners, visitors and assets to the extent agreed by your Senior Leadership Team, and to provide assurance of that enhanced level. Exceeding the compliance requirements, where deemed necessary, makes sound business sense for seven primary reasons:

Continuous assurance of security

You can only address issues you can see. The board and the organization really being able to see the security situation, managing risks and measuring security performance, is what leads ultimately to continuous assurance of security.

Certainty of compliance

Compliance is still as important as ever. A SeMS doesn't change that but it does improve how compliance is achieved and assured. Precisely because risks are being managed and performance is measured, management has certainty of compliance, sees deviations and can fix them in good time. No surprises, no preparation needed for regulatory inspections.

Security is improved

More certainty about security performance, and a much fuller picture of risks, not just snapshots, lead to improved security.

Fulfills duty of care

As custodians on behalf of the shareholders, directors have a duty of care for the security of staff, customers, the public and the business itself. A robust SeMS equips directors to fulfill that duty: it protects the organization from security-related business risks, and people from harm.

Dispels abundance of caution and reduces waste

Organisations often say they are taking action out of an "abundance of caution". What that usually means is, "We don't really know how secure we are". This 'Just in Case' attitude is wasteful: with greater assurance and more confidence in the organization's security measures, it becomes possible to target resources better at where they are most needed and eliminate 'Just in Case' activities. That means lower costs for the same level of security; in other words, reduced waste and increased productivity. It also means the disruption and the secondary risks caused by unnecessary precautions are avoided.

Nurtures a positive culture

The SeMS nurtures an environment where security is regarded as important and everybody's responsibility, helping to generate a collaborative approach by engaging the workforce. The SeMS framework highlights the importance of this positive security culture and every component, every chapter of the framework, helps to nudge the security culture forward. One practical example is the effect of eliminating 'abundance of caution': people appreciate they are no longer expected to do tasks they have always known were pointless, which nudges the culture forward.

Saves money

Productivity improves, with direct financial benefit. Minimizing unplanned work to deal with incidents and avoiding emergency remediation work clearly reduce costs. Unplanned work is always more costly than planned, so better to be guided by your SeMS to do it right and prevent those surprises.