SeMS Innovation Report: making security a strategic capability

Introduction

Why do security breaches happen?

With the benefit of hindsight, the US Government Commission reporting on the 9/11 attacks said:

> "*We believe the 9/11 attacks revealed four kinds of failures: in imagination, policy, capabilities, and management*"[1].

The aim of a Security Management System (SeMS) is to create foresight, to eliminate such failures from the organisation but the security team cannot do this in isolation. For security to be truly effective it must be embedded in the corporate management regime of the organisation.

A critical vulnerability

Every organisation is vulnerable to many threats, some with a high or catastrophic potential impact on the company. New threats continue to emerge, and existing measures often lack the agility and strategic control to respond to these in a timely manner.

If security management is not seen as a high priority at board level, this constitutes a critical vulnerability. If risk processes are weak there is little assurance that the risks on the register are in fact the most significant risks, nor that the mitigations are effective. Likewise, if the arrangements to handle a crisis are not fully formed, when the crisis comes it will be an order of magnitude more catastrophic.

Which SeMS works best?

SeMS is supremely effective if implemented properly but which version of SeMS is best? "SeMS" is just a name: people use and interpret the word differently, sometimes for valid reasons and sometimes in an unashamed sales pitch. That has led to a lot of confusion on what a SeMS actually is but the original design by the UK CAA remains the best model, and is as effective for managing all security risks in all industries as it is in aviation security.

SeMS and the organisational context

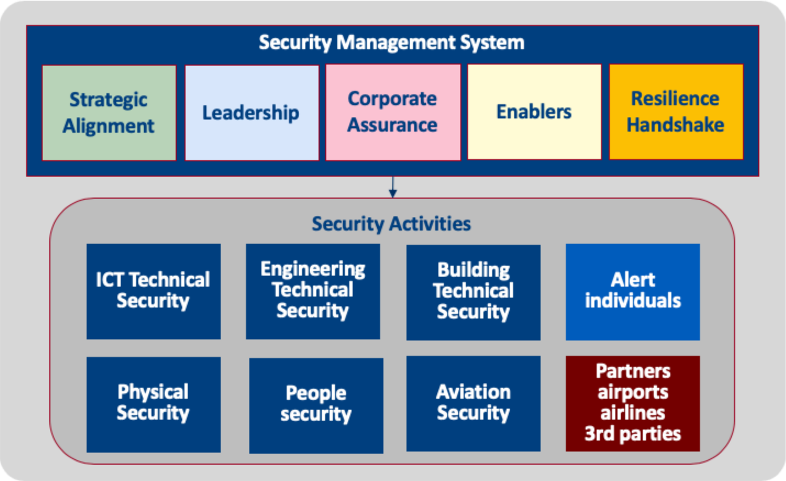
We have found that exploiting and co-operating with the existing corporate processes is the most effective solution to this critical security management vulnerability. This paper describes a SeMS integrated into the corporate context, creating the ability to respond strategically, tactically and operationally as needed.

Making security a strategic capability

The CAA's *SeMS Framework*[2] is an excellent model for security management but necessarily excludes other corporate systems with which a SeMS should dovetail. The 3DAssurance team has updated the framework so that SeMS becomes a strategic capability[3] , a corporate means of managing security risks, incidents and crises. It makes security a company-wide priority, addressing existing vulnerabilities and weaknesses and equipping the organisation with the wherewithal to respond to future risks, incidents and crises robustly and quickly, at the right level in the organisation.

The updated SeMS is made up of five themes, based on the UK CAA *SeMS Framework*; on the FEMA Report *Crisis Response and Disaster Resilience 2030*[4]; and on *Doughnut Economics*[5] by the economist Kate Raworth. It also draws heavily on corporate governance good practices.

The themes are:



- **Strategic Alignment** to business goals to address *Failures in Policy*
- **Leadership and Direction** to address *Failures in Management*
- **Corporate Assurance** to address *Failures in Imagination and Capabilities*
- **Enablers** to address *Failures in Capabilities and Management*
- **Resilience Handshake** to address *Failures in Imagination and Capabilities* in security's support of Resilience and Crisis Management

Benefits

There are four quantifiable benefits.

1. SeMS prevents surprises, whether from known risks inadequately mitigated or failure to identify risks. Unplanned responses are inevitably more costly than planned activity, error-prone from urgency, and carry the risk of unpredicted consequences.
2. The improved capability reduces the cost of risk, by reductions in probability and impact of risks, and in the duration of incidents and crises.
3. Security costs are more flexible and can be reduced by using a better understanding of the risks to avoid 'Abundance of Caution' in preventive and reactive measures. Additionally, the ability to get risk responses right first time reduces wasted effort and re-work as well as accelerating the resolution.
4. Greater risk assurance enables the Board to make future investment and strategy decisions with more certainty and business opportunities are less likely to be rejected through lack of confidence.

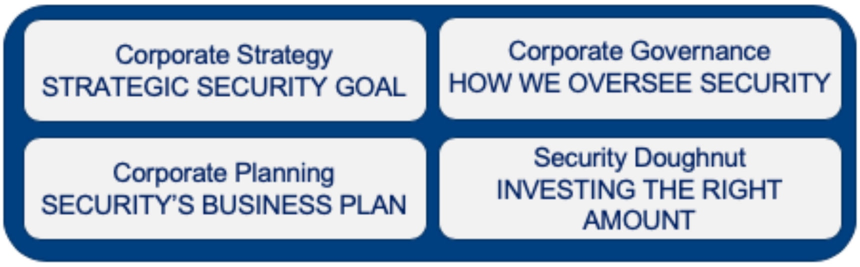
In addition, SeMS equips directors to fulfil their duty of care: it protects people from harm, the organisation from risks, and the shareholders' physical, reputational and goodwill assets.

Finally, the SeMS culture, in which risks are regarded as everybody's responsibility, helps to engage the workforce in collaborative working and encourages security-mindedness.

Costs

The cost of development is relatively small, using mainly in-house resource plus a small amount of external resource for guidance and quality assurance. The opportunity cost of seconding in-house managers and staff onto this project is the most significant element of cost, and is managed like other strategic projects by including it in the corporate business plan, allocating resource according to the company's goals and risk appetite.

1. Strategic Alignment to business goals


Corporate Strategy
STRATEGIC SECURITY GOAL

Corporate Governance
HOW WE OVERSEE SECURITY

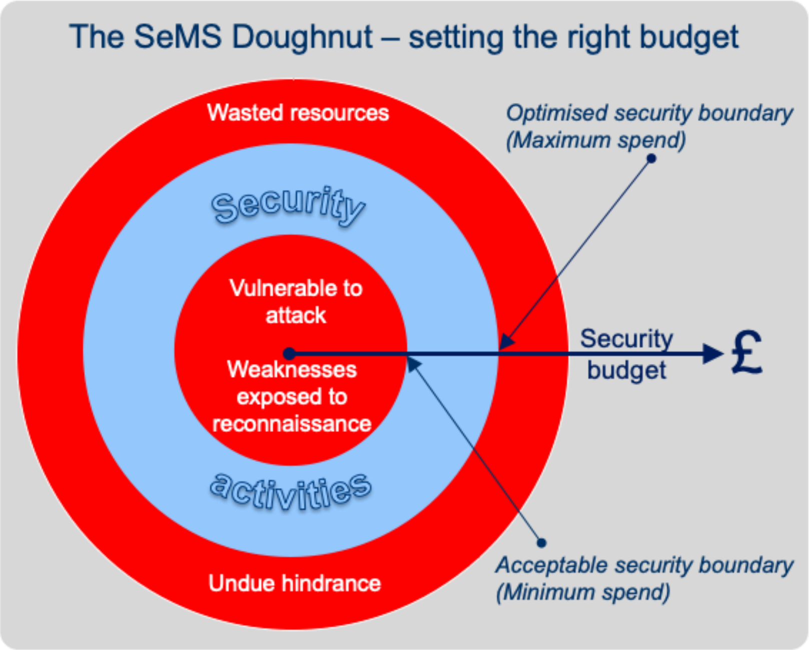
Corporate Planning
SECURITY'S BUSINESS PLAN

Security Doughnut
INVESTING THE RIGHT AMOUNT

Security Policy should be a strategic corporate policy, not a policy just for the specialists. Like other core activities, the SeMS should be aligned explicitly to the company's strategy and corporate plan. **Corporate Strategy** sets the organisation's direction and should include a security goal to deliver and improve security risk and management in a way that best supports the company's business goals.

Building security in as a core activity in the **Corporate Planning** process ensures it is fit for the corporate purpose and supports the company's business goals with appropriate and proportionate risk responses. It also binds together the security silos – cyber, physical, people and perhaps more. Each security discipline has its own procedures, skills and tools, but working in isolation creates gaps through which issues may fall. Silo working is not a specialist's instinctive behaviour, it is driven by the hierarchical separation of departments into technical divisions, ICT, HR, Property and others. Strategic alignment of the SeMS through the Corporate Plan provides the organisation-wide perspective with overarching shared strategic security goals for all security disciplines.

Security spend will be guided by risk assessment, neither too low nor too high. Key to this is the SeMS Doughnut. The **SeMS Doughnut** enables the corporate governance regime to manage the proportionality of the security investment with a cost-benefit analysis based on the concept of *Doughnut Economics*[3], a model of a self-sustaining balanced economy, in which resources are applied where they are needed, waste is prevented and constant inflation of cost is unnecessary.

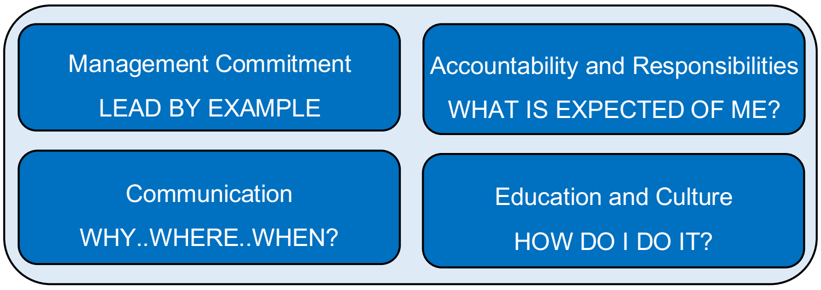

The SeMS Doughnut – setting the right budget
Wasted resources
Optimised security boundary (Maximum spend)
Security
Vulnerable to attack
Weaknesses exposed to reconnaissance
Security budget
£
activities
Undue hindrance
Acceptable security boundary (Minimum spend)

The correct risk investment is a balance of financial and opportunity costs against benefits, with margins to allow for error in the risk assessments and the control of performance. Under-investing in security is clearly dangerous, leaving risks unmitigated. However overspending on security, "Abundance of Caution" as it is often called, has equally undesirable downsides, not only in unnecessary expense, but in opportunity costs such as shying away from new business opportunities, or increased customer inconvenience and dissatisfaction.

The doughnut model enables business planners to assess the consequences of both over- and underspend and thereby identify the optimal spend, the investment that is both *necessary* and *sufficient* to optimise security.

These measures automatically bind security into **Corporate Governance** which directs and oversees the management of all other business processes including corporate risk.

2. Leadership and Direction



Management Commitment
LEAD BY EXAMPLE

Accountability and Responsibilities
WHAT IS EXPECTED OF ME?

Communication
WHY..WHERE..WHEN?

Education and Culture
HOW DO I DO IT?

The SeMS is not a mechanistic system. It provides the controls and processes, but they cannot operate without people. *Direction* ensures people are clear about the corporate security goals, and *Leadership* ensures they are committed to delivering them – essential for maximising effectiveness and minimising wasted effort and time, and for staff morale, the "winning team" mentality.

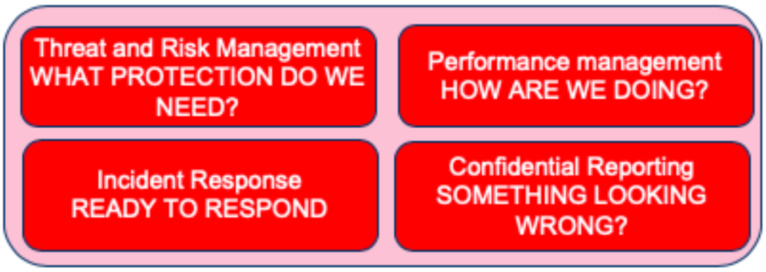
Failures in management are evidenced by uncommitted staff who do not understand their roles and have no faith in their chain of command – they are being administered but not led or directed.

Management Commitment to the SeMS regime is demonstrated by all levels of manager leading by example, leaving people in no doubt about the importance of security and resilience, in particular the identification and management of risks, and reporting issues.

If **Management Commitment** establishes the security ethic through leading by example, **Accountability and Responsibilities** explains to people what is expected of them, their roles and their accountability for risk, including roles that are not part of the direct security operations. It gives them direction. And through the Just Culture policy it holds staff and contractors accountable for their actions, treating genuine mistakes with understanding whilst protecting the company from deliberate malicious acts with proportionate sanctions. People also need the knowledge and skills to know *How* to fulfil their responsibilities. **SeMS Education** provides the requisite skills and explain the principles behind SeMS.

All this is backed up with **Communication** to keep risk awareness high and reinforce **Management Commitment** with updates and refreshers.

3. Corporate Assurance



Threat and Risk Management
WHAT PROTECTION DO WE NEED?

Performance management
HOW ARE WE DOING?

Incident Response
READY TO RESPOND

Confidential Reporting
SOMETHING LOOKING WRONG?

The primary goal of the SeMS is to manage risks, maintain effective crisis and incident response measures, and assure the board that security is under control.

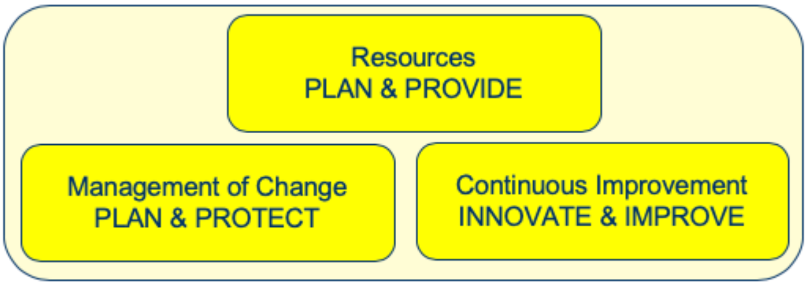
Threat and Risk Management is the core of the SeMS. Robust and effective risk monitoring ensures that proportionate controls are allocated to risks, neither exposing the company beyond the board's risk appetite, nor unnecessarily cautious, restrictive or expensive. A cross-company Risk Review Group of senior staff and managers ensures risks are properly identified, understood and assessed, and allocates responsibilities right across the business. The mission of this group is the foresight to avoid any failure of imagination in anticipating risks, recognising the potential impact of anticipated risks, or in identifying effective mitigations.

Incident Response ensures any risk that materialises is dealt with effectively and lessons are learnt to prevent recurrence or improve the response. It provides an escalation path for operational to tactical incident management, and when the incident escalates beyond routine management, to Crisis Management (Theme 4).

The **Confidential Reporting** scheme enables staff to report concerns and receive feedback on how those concerns have been addressed. Some concerns may alert the organisation to previously undetected vulnerabilities, threats or risks, including insider threats.

Underpinning all these, **Performance Monitoring** measures security performance and SeMS effectiveness to provide continuing assurance that risks are under control. This includes quality assurance of all SeMS capabilities.

4. Enablers



Three processes support the operation of the SeMS, protecting it from failures in the key capabilities.

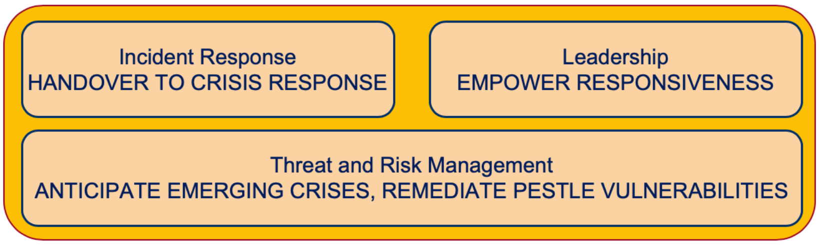
Inadequate resource is one of the main threats to effective security. **Resource Provision** ensures that the right amount, type and quality of resource (including contracted services and products) is allocated to each activity, to ensure the balance between resourcing and exposure that Threat and Risk Management intended is achieved, and is delivering the intended protection.

A stable security regime is at risk from changes external to the SeMS. **Management of Change** ensures that operational, organisational, physical, system or functional changes do not have an unplanned impact on the company's security or SeMS.

Continuous Improvement empowers people to identify and try out opportunities to improve the SeMS. This is not about saving money, it's about doing security better.

It also provides protection against evolutionary decay. The organisation and the business environment are not static, and even small changes may compromise the effectiveness of security capabilities. A change to the business operation or its context may create opportunities to improve those capabilities and restore their effectiveness.

5. Resilience Handshake


Incident Response
HANDOVER TO CRISIS RESPONSE
Leadership
EMPOWER RESPONSIVENESS
Threat and Risk Management
ANTICIPATE EMERGING CRISES, REMEDIATE PESTLE VULNERABILITIES

Resilience is not a SeMS capability. It is a corporate provision not restricted to security crises, but for the management of all emergencies that exceed the control afforded by defined processes. However a security incident may escalate to a crisis, or a non-security crisis may have a security impact, so SeMS provides for a smooth handover into the Crisis Management 'process' via the Resilience Handshake theme. Whilst

Incident Response is the primary interface with Crisis Management, there are proactive SeMS+ components that support other aspects of Resilience too.

Incident Response

A crisis is an event for which there is no pre-determined routine solution. It will often start as an incident, and when it escalates beyond routine management, it is escalated to Crisis Management. In the case of security incidents, **Incident Response** provides the escalation path to Crisis Management when needed.

Leadership

Top management is responsible for the organisation's **Crisis Response**, directing the Crisis Management Centre (CMC). The CMC's role is to be the control centre, reacting quickly, managing available information and outgoing messaging, triaging and making decisions at the right level in the organisation, implementing crisis measures promptly in collaboration with external partners and authorities. This relies on **Management Commitment**, **Communication** and **Accountability and Responsibilities** to empower people's response, equipping them to use their intuition and experience to make and change decisions despite incomplete and conflicting information; and to provide **Education** with models, scenarios, and simulations to tease out stress points and gaps and address them. The Resilience Handshake also draws on the Leadership theme to develop a culture of foresight by building a shared vision of the future and a culture that embraces forward thinking, not only for managing crises, but also to enhance all aspects of Resilience planning.

Threat and Risk Management

Threat and Risk Management supports Resilience by:

(a) Anticipating emerging challenges and developing appropriate plans and contingencies
(b) Modelling alternative scenarios to meet the interdependent challenges of PESTLE[6] factors
(c) Determining and remediating supply chain vulnerabilities particularly for infrastructure services in anticipation of both global and local supply challenges.
(d) Identifying crises at the earliest opportunity, whether by escalation of major incidents, monitoring leading indicators and other warning signals for impending crises, using open and closed information sources, social media or other means.
(e) This includes understanding and remediating potential points of catastrophic failure. Crises can escalate into catastrophes when consequences are not addressed and compound each other – the 'snowball effect'.
(f) Managing changes in customer and partner capabilities.

Summary and Elevator Pitch

The updated SeMS is a framework to manage security corporately, to bring an organisation's security management into the core of the business as a strategic capability, supporting the business's sales, marketing, operations and resilience goals. It is based on proven, simple concepts and methods that ensure the best possible response to risks, incidents and crises, minimising the chaos, damage and harm that might otherwise be caused.

References

[1] 9/11 Commission (2004) *The 9/11 Commission Report Chapter 11* https://govinfo.library.unt.edu/911/report/911Report

[2] CAA (2018) *SeMS Framework* https://publicapps.caa.co.uk/modalapplication.aspx?appid=11&catid=1&id=6543&mode=detail&pagetype=65

[3] Deloitte (2015) *Strategic capabilities* https://www2.deloitte.com/ie/en/pages/consulting/articles/strategic-capabilities.html

[4] FEMA (2012) *Crisis Response and Disaster Resilience 2030: Forging Strategic Action in an Age of Uncertainty* https://www.fema.gov/media-library/assets/documents/24174

[5] Kate Raworth (2017) *Doughnut Economics* Penguin Random House, London

[6] CIPD (2020) PESTLE analysis https://www.cipd.co.uk/knowledge/strategy/organisational-development/pestle-analysis-factsheet