Achieving Assurance in an Uncertain World – How SeMS helps

Andy Blackwell, former Head of Security with Virgin Atlantic and now a Registered Independent Security Consultant specialising in Transport Security, looks at how Security Management Systems (SeMS) help airports, airlines and other aviation entities achieve assurance of their security robustness.

Background

The evolution of terrorist threats targeting civil aviation assets has again been highlighted by the authorities. Additional security measures have been implemented in several locations with the prospect of the requirements being extended to other areas. Recent history aptly demonstrates the unhealthy interest Islamist terrorists, and those inspired by them, retain in civil aviation with attacks (including attempts), against the industry being conducted in Egypt, Belgium, Somalia and France. Plots have been directed at 'hard' and 'soft targets' and included air and ground assets, in an effort by the perpetrators to inflict mass fatalities, create a climate of fear, disrupt transport infrastructures and cause significant economic damage.

The frequently used, but still relevant quote *"We only have to be lucky once. You will have to be lucky always"* used by the Provisional IRA following their plot to kill Prime Minister Margaret Thatcher and members of her cabinet who were using the Grand Hotel in Brighton in 1984, is still relevant today. It's not about being consistently lucky though, but more appropriately being assured that our security arrangements are robust and able to deter, disrupt, detect and respond to targeted attacks against people and assets.

The need for assurance of aviation security defences cannot be overstated, to help the industry manage a dynamic, challenging and evolving threat landscape. Security Management Systems, or SeMS for short, have a key role to play in helping security-assure the industry.

In this article "Compliance" refers to compliance with any fixed requirements, not only the regulations. In unregulated circumstances, there can still be a tendency to think that the protective measures are fixed and that the aim is just to ensure full execution of those measures. The point of SeMS, in unregulated as well as regulated industries, is to avoid "fixed" thinking by continually reviewing the ever-changing risks and instituting new and changed measures accordingly.

Security Management Systems - implementation and development

Security Management Systems (SeMS) are based on the industry's success with Safety Management Systems (SMS). Some aviation entities combine their safety and security systems into an overall 'management system'. The International Air Transport Association (IATA) has for many years required member airlines to have an effective SeMS, and the UK's Department for Transport and Civil Aviation Authority have worked and continue to work closely with airlines, airports and cargo entities to develop and implement SeMS across the industry. The scheme is voluntary now, but early adopters report significant benefits and the increased take-up across the industry is encouraging. The UK's Centre for the Protection of the National Infrastructure (CPNI) has also been working with key Government and Industry stakeholders to identify the benefits SeMS could bring to the UK's critical national infrastructure (CNI).

Whilst the concept of Safety Management Systems (SMS) is well established, there does appear to be a lack of understanding in some parts of the sector as to what a Security Management System (SeMS) actually is. The term has many different uses and misuses but in simple terms, SeMS is a management system and most professional organisations will, if they don't already have an integral SeMS, have many of the components to enable them to 'assure' security within their businesses. The formal definition of a SeMS (UK DfT/CAA) is *'an organised, systematic approach to managing security that will help embed security into an organisation's day to day management operations and general management systems. It provides the necessary organisational structure, accountabilities, policies and procedures'.* This definition reinforces the concept that security is not a bolt-on, but should be an integral part of everything the organisation does, as an enabler, not a constrainer of business.

There are ten chapters in the DfT/CAA's Framework for an Aviation Security Management System (SeMS) CAP1223 which cover the following key areas:-

Management commitment
Threat and risk management
Accountability and responsibilities
Resources
Performance monitoring
Incident reporting
Management of change
Continuous improvement
SeMS training
Communications

The success of the UK DfT/CAA SeMS 'product' is largely because it has been developed jointly with industry which has helped to make it practical, relevant, and straightforward to implement. The value of the discussions between regulators and industry representatives during the early stages of the project was mutually beneficial and continues to be most valuable as the project progresses. Regulators and industry have the same objective; a safe and secure aviation industry.

SeMS Myths, Rumours and Legends

There are several myths circulating about SeMS which this article aims to dispel.

1. A SeMS is a manual and it will end up with all the others on the shelf.
No, SeMS is a dynamic process which if implemented and used correctly will enable continuous improvement. By its very nature SeMS is future-proofed.

2. A SeMS is expensive
Additional funding is not always necessary when starting the SeMS journey, as many entities will already have many of the component parts needed for an effective SeMS.

3. A SeMS will magically solve our security problems
It won't but it will give much needed greater visibility of security risks and compliance performance.

4. *SeMS is a one-size fits all concept*.
SeMS is adaptable: it has a framework, but it's not a rigid process. It's designed by the organisation for the organisation.

5. A SeMS is an IT system
It is not an IT system per se, but IT Security Operations Centres could certainly form part of it, and there are specialist software applications that would complement an effective SeMS.

6. A SeMS will hinder us.
From the experiences of early adopters of SeMS, the concept is very much seen as an aid to security management, not a burden.

7. A SeMS removes the need for compliance
From a regulatory point of view, it's important to stress that SeMS doesn't remove the need to comply with statutory requirements, it makes it easier for organisations to evidence their compliance and assurance activities. Whilst the rollout of SeMS is unlikely to change the way regulators audit, they will have greater data at their disposal. If SeMS is adopted by a substantial proportion of the industry, regulators could move progressively into what is often called performance based oversight.

A SeMS should be built around an assessment of risk to the organisation and its ability to assess the impact. Risk represents challenge and opportunity and therefore requires careful management. If we overreact to all possible risks, we could create threat fatigue and encourage hoaxes against us e.g. bomb threats, and conversely if we underreact we may be creating the path of least resistance that terrorists could exploit. The more we understand the effectiveness of our security assurance and delivery, the easier it is to make informed judgements about threat and risk. The risk assessment 'tools' in an effective SeMS enable organisations to prioritise their vulnerabilities and sensibly deploy resources to help mitigate risks.

Benefits of a SeMS The benefits some early adopters have achieved include:-

Creates Board level accountability for security, an Accountable Manager able to allocate funds and resourcing, supported by a Security Manager who is a security subject matter expert.

Enables the Board to monitor their organisational wide levels of security assurance and set their own metrics.

Helps organisations demonstrate they are discharging their accountability and responsibilities for security

Encourages transparent and verifiable security – there shouldn't be any surprises. An effective SeMS will identify good performance and areas where additional focus may be required.

Delivers greater visibility of compliance assurance – it's not just about an organisation saying they are compliant, but having the ability to demonstrate this. This should make regulatory audits more productive enabling mature discussions to take place.

Enables more effective use of existing tools and systems – SeMS is not about creating something new, but making more effective use of the tools and processes already in place.

Supports risk management and enables confidence levels of existing security arrangements to be accurately assessed – this in vital in today's threat landscape.

Builds on SMS learning as opposed to 're-inventing the wheel'. There is a much 'learning' available from the development of SMS that is transferable to SeMS.

Encourages collaborative approaches with regulators and other industry stakeholders.

Empowers and promotes pro-active reporting – the 'lifeblood' of SeMS.

Drives a more assurance based regime as opposed to pure compliance.

Creates a more sophisticated and holistic approach to security assurance and organisational resilience – whilst the original concept of SeMS was to help entities assure themselves that they were meeting the mandated security requirements, organisations are able to expand their SeMS to cover all organisation wide security activities, thus providing them with a much richer threat and security risk picture.

SeMS Learning

The learning from early adopters highlights that it's not necessary – nor desirable – to compile a specific SeMS manual, as most entities will already have documented processes that will in reality be the core of their 'SeMS'. Using the manual to sign-post documents was found to be the major benefit, showing references to where key information could be found. A common error when embarking on the SeMS journey was trying to second guess what the regulator wanted to see in terms of output, rather than focusing on what the Board needed to know to assure themselves.

Entities reported that the more they joined up the various components of SeMS, the greater their assurance picture became. To illustrate this, one organisation said that at the start of the SeMS process it was like looking at jigsaw pieces in a box, all the pieces were there, but until joined up you couldn't see the complete picture. Another memorable description was that the assurance picture pre-SeMS was like vision with cataracts but as the system developed and more components were matured the view became 20/20. The comments have a common theme and demonstrate that an entity's assurance picture becomes much clearer with an effective SeMS.

Organisations reported that SeMS had changed behaviours within their businesses, with an increased focus being placed on security. It has also encouraged greater collaboration with regulators and other key stakeholder, with some organisations conducting joint inspections and audit activities. There has also been much sharing of best practices, and knowing what others do well in terms of security certainly helps ensure the overall integrity of aviation security.

Collaboration Opportunities

The development of SeMS is also creating collaboration opportunities. Whilst SMS was originally intended for airlines, SeMS was designed from the outset for the whole industry. Some airports and cargo entities are now adopting SeMS, with interest also being shown from industries forming part of the critical national infrastructure. The SeMS framework is flexible enough to be used in a wide range of organisations and the more SeMS there are in place the greater the overall security-assurance picture will become.

Looking at the aviation-industry and in particular the airport environment, SeMS could be implemented and add value to the following organisations:-

Airports
Airlines operating to and from the airport in question
Cargo operators and freight forwarders
Supply chain, including catering and inflight supplies
Handling agents
Other transport modes (e.g. rail and other land transport) servicing airports
Hotels situated within the airport estate or its vicinity.
Critical national infrastructure
Retail facilities
Policing/regulators

There is also the potential to link the SeMS of various entities which would provide a broader assurance view and a more joined-up approach to overall security delivery.

Conclusion

With the ongoing and evolving focus on the aviation industry by those with sinister intent, there has never been a greater need to ensure that our security management and assurance systems remain fit for purpose and help us identify and mitigate new and emerging threats and risks. Implementation and development of SeMS will enable entities to continue to ensure the integrity of aviation security and demonstrate they have robust oversight in a dynamic environment, far beyond what compliance alone provides. The development of measures of performance and effectiveness is key and will help organisations to evaluate the impact of their deployed SeMS, demonstrate a proportionate focus and validate that things are improving as expected.

Andy can be contacted via andy@blackwell-security.co.uk *His website is* http://www.blackwell-security.co.uk *and twitter feed @bsc_secure*

Andy Blackwell
Managing Director
Blackwell Security Consulting