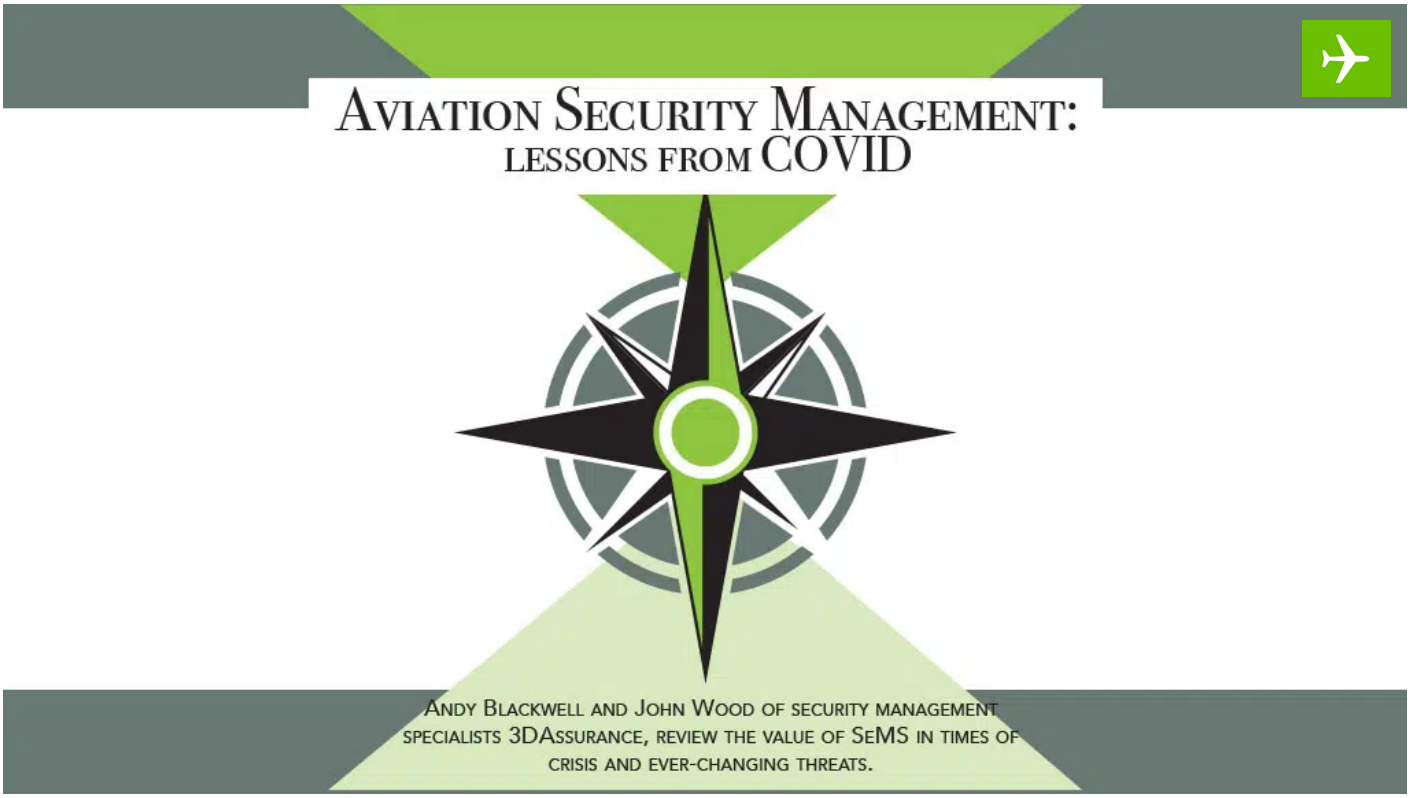


AVIATION SECURITY MANAGEMENT: LESSONS FROM COVID

Oct 3, 2021

The aviation sector is no stranger to crises, from lethal attacks at airports and against aircraft in flight to safety issues, accidents and natural events such as volcanic ash clouds. The COVID-19 pandemic is the latest crisis to affect civil aviation and is potentially the most challenging the industry has ever faced. As the sector begins to recover, it continues to face a complex and dynamic threat landscape requiring a relentless focus on threat and risk

ongoing COVID-19 challenges, terrorism, cybercrime and insiders remain potent threats, the nature of which the pandemic has adversely affected.

THE THREAT LANDSCAPE

The detection in July 2021 of a viable improvised explosive device concealed in a musical instrument and intended to be detonated by a passenger on a domestic flight in Afghanistan, together with suicide bomb attacks in the vicinity of the Hamid Farzai International Airport highlight the unhealthy interest terrorists retain in civil aviation. Terrorist activities by ISIS, AQ and their affiliates have largely continued unabated during the pandemic despite the reduced availability of some targets and severe restrictions on international travel.

The cyber threat continues to grow due to the sector's increased connectivity and as more aviation related activities become virtual, industry is finding it difficult to keep pace. The sector is attracting persistent attention from cyber criminals too, keen to exploit the data within the industry. Hybrid threats have been accelerated by Covid and involve attacks against aviation systems to facilitate physical harm to people and assets. Such attacks include disabling critical national infrastructure, and the creative targeting of aviation such as offsetting navigational aids and disabling of CCTV systems over IP networks. The vast array of systems the sector uses provide an additional threat vector and a target rich environment for those seeking to cause us harm. Nation states, extremists and organized crime groups have long known and exploited the benefits insiders can bring to advancing terrorist plots and criminal endeavours. The pandemic has increased people risks in the sector due to the significant number of employees made redundant, furloughed, or working remotely, many of these possessing unique knowledge. Many of the potential insiders are now outsiders. The UK's National Crime Agency recently issued an alert warning that furloughed port and airport workers were 'at risk of corruption' by organized crime groups. Cyber-based 'insider threats'

interconnectivity between cyber and physical systems can create an increased risk of accidental and deliberate disruption by these individuals. In addition, some of those retained by the sector have been employed on lower salaries and reduced benefits. The potential for disgruntlement is high and the level of industrial action within the sector reflects this. The recruitment pool available to terrorists and other bad actors has increased significantly.

The early identification of warning signals and timely remedial action is key to protecting against aviation security incidents, and hybrid threats and the potential distraction caused by COVID have made this harder. Hybrid threats increase the risk of warning signals being missed, but there is an even more fundamental issue: where warning signals are being seen they are not always acted on effectively. Too often, aviation security risk registers identify cyber threats, but these are carried over from one meeting to the next because the risk managers do not have the relevant experience, training or support to understand and manage the risk effectively.

Security Management Systems have proved their worth in the pandemic – one regulator reporting that organizations with a SeMS fared better than those without – and can rise to the challenges aviation security is now facing.

This section outlines the SeMS functions so that later sections can discuss how they address the hybrid threat challenge and also improve resilience as business builds back post- pandemic. For a detailed description we recommend the CAA SeMS Framework (search for CAP1223 on caa.co.uk) or the ICAO version, in Chapter 9.3 of the Security Manual (Doc 8973).

The purpose of the SeMS is to give top management Corporate

key components:

1. 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. Proportionality is essential: foregoing business opportunities or burdening staff and customers with unnecessary controls through fear of risks that are in fact tolerable, is as undesirable as taking undue risks. A cross-company Risk Review Group made up of business, operational and security people ensures risks are properly identified, understood and assessed. Its mission is to anticipate risks, recognise the potential impact of those anticipated risks, and instigate effective mitigations.

2. Incident Response ensures any ad-hoc threat is dealt with effectively and lessons are learned to prevent recurrence or improve the response. It provides a "resilience handshake" and escalation path when the incident grows beyond routine management, to Crisis

outside the SeMS.

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

4. Performance Management measures security performance and SeMS effectiveness to provide continuing assurance that security is strong and risks are under control.

However, a SeMS is not just a mechanistic system. It has five Leadership and Direction components essential for developing a positive Security Culture, maximising the effectiveness of the SeMS and creating a "winning team" mentality.

1. 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.

2. Accountability and Responsibilities explains to people

and their accountability for risk, including roles that are not part of the direct security operations.

3. The Just Culture policy holds people accountable for their actions, treating genuine mistakes with understanding whilst protecting the company from deliberate malicious acts with proportionate sanctions.

4. SeMS Education provides the knowledge and skills people need to fulfil their responsibilities.

5. All this is backed up with regular Communication to keep risk awareness high and reinforce Management Commitment.

Finally, there are three Enabling components.

1. Resource Provision ensures that the right amount, type and quality of resource (including contracted services and products) is allocated to each activity.

2. Management of Change ensures that operational, organizational, physical, system or functional changes do not have an unplanned impact on the company's security or SeMS.

empowers people to identify and try out opportunities to improve the SeMS. This is not about constantly raising the bar of security performance, it's about refining the processes so that they work smoothly and without fail in all circumstances, even in a crisis.

SEMS: A NEW KIND OF VIGILANCE, A NEW WAY OF WORKING

It is clear we need a new kind of vigilance and a new way of working. Security teams tend to work in silos because that is how the organization manages them, with different reporting lines, objectives and incentives; and tend to have their own jargon because that is how the industry speaks to them. Both these barriers need to be broken down, but it is unlikely that we will see a hybrid cyber/physical security team any time soon. Instead, we need to create the environment and forum in which they can work closely together.

Organizations have management systems and governance frameworks to control the delivery of corporate objectives through

and risk management and these can be extended without compromising them.

To create an environment in which security collaboration thrives, an organization should specify "collaboration objectives" — creating, monitoring, and funding departmental objectives that mandate collaboration across departments to facilitate their shared responsibility for delivering corporate security objectives.

These governance changes will remove the obstacles, but further work is required to establish active collaboration between the security teams.

The Threat and Risk Management process should be extended to include Cyber and Enterprise Risk teams in the Risk Review Group and drive collaborative discussion of all views and assessments to form a fully rounded picture of all threats and risks, physical, cyber and hybrid.

Thoughtful application of the SeMS Framework will evolve common, overarching management systems aligned across the disciplines. Its simple yet comprehensive structure

approach to managing threats and risks regardless of whether they are the physical, infosec or enterprise team. It will identify the interactions between the teams and implement integrated ways of working at that common overarching level, without compromising the individual practices, techniques and skills of each security discipline.

SEMS: A NEW KIND OF RESILIENCE

Covid-19's effect on aviation has been as devastating as the virus itself. Organizations have been presented with new challenges and opportunities, prompting business leaders to pose the question: "What do we need to do to become a highly resilient organization?" Those who get the answer right will not just survive future crises, they will have created the conditions to thrive. A failure of imagination in this regard will result in a very predictable outcome. As other crises loom, time is of the essence. Security and resilience need to be integral parts of an organization's corporate culture.

where a SeMS has improved security as intended, but one of the perhaps unexpected lessons from the pandemic is that SeMS improves resilience.

We think that is not only because of that resilience handshake between Incident Response and Crisis Management, we think the whole of the SeMS had a part to play. In threat and risk management, warning signals were recognized earlier because the focus was not simply on regulated risks.

The Security Culture meant that people felt their responsibility, took the initiative and did whatever had to be done.

Communication was clearer because everybody knew their responsibilities and how to take action. In particular the incident response process was fully formed, it was ready and tested so that the response was quick and effective.

The resilience handshake in Incident Response ensured escalation to crisis management ran smoothly, and Crisis Management itself was ready. This is particularly interesting because Crisis Management is a SeMS itself. We think that may be because organizations that adopt a SeMS become generally more systematic and process-focused: they had robust processes that were properly understood and had been well practiced. We call this security as done as opposed to security as imagined.

Security as imagined is what is written in the procedure manual but when the operation gets stressed by external circumstances like the pandemic, people find shortcuts and what they think are better ways of doing things. A well-established SeMS will already have done this refinement through Continuous Improvement so there is no need to deviate from the procedure manual in times of crisis: it already incorporates Security as done.

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

Leadership and Direction enhances people's ability to respond in a crisis, equipping them to use their intuition and experience to make or

and conflicting information, and provides Education with models, scenarios, and simulations to tease out stress points and gaps and address them.

Threat and Risk Management supports Resilience by anticipating emerging challenges, remedying vulnerabilities and developing appropriate plans and contingencies ahead of time.

Andy Blackwell is a subject matter expert on SeMS and a wide range of transport security matters. He provides support to the UK CPNI's SeMS Study and consultancy to the UK Department for Transport. Blackwell was formerly Head of Security with Virgin Atlantic, where he was responsible for all aspects of the airline's security Management Systems (SeMS) implementation and development. In that role, Blackwell was the leading industry contributor to the development of the UK SeMS Framework. He took a primary role in the government-industry working group that reviewed and contributed throughout the Framework's development; he drafted some parts of the Framework and associated documents; and he put the Framework into practice, implementing it successfully at Virgin. Prior to joining Virgin Atlantic, Blackwell was UK security manager and lead threat assessor with DHL. Blackwell has a law enforcement and intelligence background, with previous service with UK Customs, British Transport Police, the National Criminal Intelligence Service and the National Drugs Intelligence Service of the Czech Republic. Blackwell is now managing director of Blackwell Security Consulting. He is a Registered Independent Security Consultant with the Association of Security Consultants and member of the Advisory Boards of UK Security

Review. Blackwell is a regular speaker at international security events and has authored numerous published articles on SeMS and other security-related topics.

John Wood is a Security Management Systems (SeMS) subject matter expert, and was responsible at the UK CAA for developing the UK SeMS framework published jointly by government and the CAA. As the CAA's Aviation Security Strategy Lead and SeMS subject matter expert, Wood worked with many industry stakeholders and guided the first two pathfinder organisations to develop their SeMS to achieve a successful regulatory assessment. Experienced in guiding the design

strategic change in public and private sectors to improve operational effectiveness, Wood has been a lead designer of numerous governance, risk and compliance systems. He is adept at unifying strategic vision with its practical delivery to drive business change and align objectives with business requirements; innovating practical solutions to strategic and operational challenges, removing obstacles to change and achieving strategic goals and training / mentoring multi-disciplined teams to embed fresh working practices and behaviours which drive performance improvements. Wood is a qualified project, program and risk manager, (PRINCE2, MSP, MoR) and holds a masters degree in Physics from Oxford University.

NOW IS THE TIME

It should be no surprise that SeMS offers robust solutions to post-pandemic aviation security challenges: it is a simple common-sense approach to managing risks, harnessing proven methods and techniques from the management

safety and quality.

Building a robust SeMS will ready the organization for new threats and challenges as they arise.

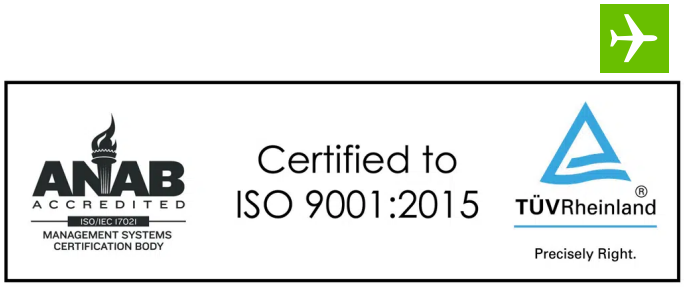
3DAssurance specializes in management systems for providing assurance that corporate risks are fully managed, with ready-made or

challenges in areas such as security, risk, quality, and safety assurance. Our team combines many years of practical experience in implementing security, risk management and assurance systems, with deep analytical and strategic design expertise.

Related Articles

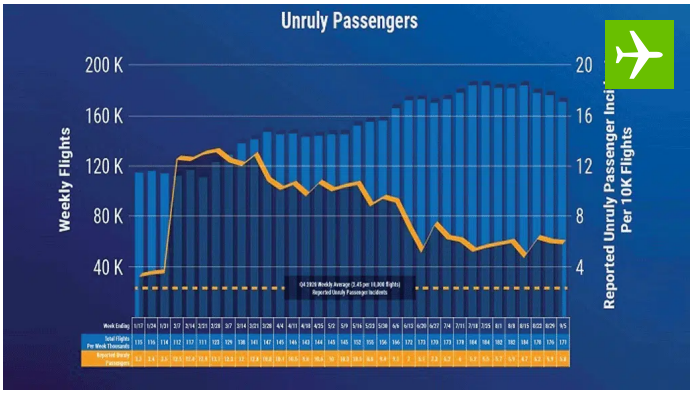
Ontic Launches New CoE Led by Threat Assessment and Protective Intelligence Investigations Expert

Joy Finnegan - Oct 6, 2021



IDSS Earns ISO 9001:2015 Quality Management Certification

Joy Finnegan - Oct 4, 2021



Drops, But Remains Too High

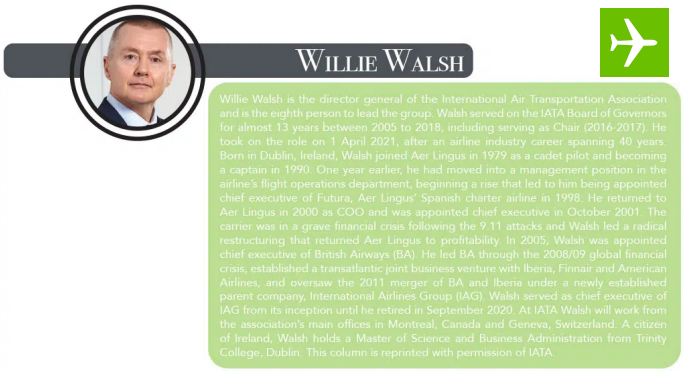
Joy Finnegan - Oct 4, 2021

9/11: SUCCESSES, FAILURES AND ENDEMIC CHALLENGES

Philip Baum - Oct 3, 2021

JETBLUE FLIGHT 261: DISTURBED INDIVIDUAL CHARGES FLIGHT DECK

David Bruce - Oct 3, 2021



REFLECTIONS ON 09.11

Willie Walsh - Oct 3, 2021