An NCC Group and 3DAssurance publication

Formation flying

Working together to protect aviation against cyber threats

Executive summary

The cyber threat to aviation is continuing to grow and the industry is finding it increasingly difficult to keep pace. Responsibility for managing the risks to business, operational and control systems is dispersed across IT security, aviation security[1] and flight safety. But the dynamic nature of cyber threats creates more attack opportunities than many realise – particularly for hybrid attacks, where a cyber intervention facilitates a physical/kinetic attack or vice versa. This increases the risk of warning signals being misinterpreted or missed altogether. A further major concern is the growth in cyber-based insider threats: the risk of accidental or deliberate disruption by individuals with legitimate access is greatly magnified by the interworking of cyber and physical systems and the potential for hybrid attacks.

In the face of these threats, close collaboration of the teams is necessary but hard to achieve. Leadership from the top and Governance, Risk and Compliance (GRC) arrangements determine how well safety, physical and cyber security teams are able to collaborate, but traditional GRC approaches are increasingly proving to be not fit for purpose. If collaboration is to be effective, a new approach is needed which enables close-coupled collaboration without requiring a wholesale change in organisation structure or GRC arrangements.

Regulations may help, but the range of regulations – including security, health and safety, financial, environmental and cyber security – tends to confuse and dilute the oversight.

Operators can enhance their aviation security defences by taking three actions based on proven techniques and frameworks that can be adopted incrementally without disrupting the business.

First, within the existing governance arrangements the various security teams' objectives and budgets, cascading to personal objectives, should be adjusted to demand and facilitate collaboration.

Second, the teams' methods and processes should be augmented with communication and collaboration mechanisms to share risk management at a high level without compromising each team's detailed techniques and skills.

Last, but very much not least, the organisation's approach to insider threats should be enhanced to include the identification, risk assessment and treatment of insider threats with the 'mainstream' aviation security risks and risk management. This will require groups not normally considered to be security focused such as HR, legal and risk management to take a more active role in securing the organisation.

> "Cyber security risk profiles are dynamic, meaning attackers are always looking to exploit vulnerabilities and can quickly develop new ways of breaching cyber security. The aviation industry's progressively interconnected systems require the industry to maintain an up-to-date awareness of both direct and indirect cyber security threats. The changing threat landscape therefore, encourages a proactive approach to cyber security and in response means aviation organisations need dynamic protection."
>
> **Cyber Security Oversight Process for Aviation (CAP1753) – UK Civil Aviation Authority**

Contents

1. Introduction 4

2. What are the challenges? 5

2.1. The warning signs are being missed or ignored 5

2.2. The nature of cyber threats creates more attack opportunities than many realise 6

2.3. The difficulty of managing hybrid threats due to silos 6

2.4. People risk is bigger than many realise 7

3. The structural challenges 8

3.1. The need for a multi-disciplinary approach 8

3.2. Weaknesses in the approach to security management 9

3.3. The means of achieving and maintaining trust needs to adapt 10

4. Rising to the challenge: The changes that matter 11

4.1. Create the conditions to facilitate collaboration 12

4.2. Weaknesses in the approach to security management 13

4.3. The means of achieving and maintaining trust needs to adapt 14

5. Now is the time 15

6. Glossary 16

7. References 16

1. Introduction

The aviation sector's threat landscape is complex and dynamic. Terrorists and other malicious actors retain their unhealthy interest in civil aviation, but it is not only conventional physical attack methods the sector has to concern itself with. Increased levels of digitalisation are attracting persistent attention from cyber criminals too, for example to exploit the valuable personal and corporate data within the industry.

However, aviation security has traditionally been a specialised function with specific tasks largely driven by regulations. This has tended to obscure two self-evident and increasingly significant issues.

First, the true purpose of security is not compliance with regulations, but protection of the business and its stakeholders from harm caused by malicious actions. That includes harm to staff, customers, the public, the environment, reputation and public confidence, as well as operations, assets and finances. Furthermore, regulations inevitably lag behind the latest innovations in security threats and organisations need to address new exposures as soon as they emerge.

Secondly, cyber security is fundamental to safe and secure aviation. With the increasing digitalisation of all aspects of aviation operations, from ticketing and inflight entertainment, to avionics and air traffic management, aviation security teams are aware of the rising threats of cyber attack but can lack the skills or resources to identify or manage them. While many recognise the importance of collaboration between the physical and cyber security teams, organisation structures and governance arrangements often create obstacles to effective cross-department working.

To understand these issues in more depth, we need to consider what 'digitalisation' implies for aviation operators, with a range of digital products including business systems; security systems; operational systems; retail systems; avionics; communication systems and many more.

Now consider which organisations or departments are responsible for specifying, procuring, developing, implementing, maintaining, using and securing each of these systems and the GRC arrangements for each: it is clear that there is little prospect of an accurate overall picture and effective oversight if these remain disjointed.

Cyber security managers may not always fully understand how bad actors could exploit cyber systems to facilitate a conventional terrorist attack on people or physical aviation assets. A siloed approach to managing aviation risks is both ineffective and inefficient. These challenges are closely aligned with the failures mentioned in the 9/11 Commission Report[2] into the deadliest attacks in the history of civil aviation, which highlighted issues in information sharing and the ways departments and agencies worked together. It is important that the increasing complexity of the threat landscape, siloed practices and the lack of a whole system approach to corporate risk management do not lead to further failures in connecting the dots and missing warning signals. The 9/11 attacks are a chilling reminder of past weaknesses in this regard.

Evolution or revolution?

Will meeting the challenges from cybersecurity require an evolution of aviation security or a revolution in how operators manage security? To answer this question, this paper outlines some key areas of concern for how the current approach to aviation security is managing cyber security risks and makes recommendations for a toolkit of comprehensive security governance and management.

We believe that the type of changes needed are an evolution of existing aviation security practices, especially given that the fundamental principles of how aviation security and information security are performed are largely analogous. However, there is no doubt that change is necessary and at a more rapid pace of change than what the industry has become accustomed to.

This is not to discount the importance of security regulations and standards, and compliance with them. However, this whitepaper is concerned with practices and processes that are not directly subject to the regulations, but form the infrastructure enabling the regulated work to be more effective. Accordingly, we reference regulations and other publications only to make specific points: for full information on the regulations readers should contact the relevant authorities and standards bodies.

2. What are the challenges?

2.1 The warning signs are being missed or ignored

Many organisations have cyber security on the risk register but are focusing on what we would call the classic "infosec" risks – data theft, fraud, ransomware and so on. Meanwhile the aviation attack surface is vulnerable to a growing variety of hybrid attacks – attacks where one or more systems are compromised to facilitate physical harm. The likelihood of warning signals being missed is increasing.

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.

Aviation security is not alone in this. For example, a pandemic has been on the UK national risk register and many corporate registers for years. A national pandemic preparedness exercise in the UK in 2016 identified potential NHS shortages as a significant risk, but problems with NHS shortages and protective equipment were still experienced during the initial phase of the Covid-19 pandemic.

Such failures of imagination and shortcomings in managing known risks are common. They are there, totally predictable, but attention to them is repeatedly deferred on the assumption they are a long way off. In The Gray Rhino,[3] Michele Wucker discusses why we often ignore the most predictable, probable threats and how, once we understand those "whys," we can do better at dealing with them instead of denying looming crises. She cites examples of these "Gray Rhinos" as diverse as the Enron collapse, climate change, the 2008 banking collapse, and the Challenger Space Shuttle, saying:

"We need to recognise that Gray Rhinos are out there – and very, very dangerous".

The cyber / aviation security threat is a Gray Rhino – out there and dangerous – but often the warning signs are being missed or ignored.

"We need to recognise that Gray Rhinos are out there - and very, very dangerous"

2.2 The nature of cyber threats creates more attack opportunities than many realise

The nature of cyber attacks means that it is unwise to assume risks are of low likelihood given active adversaries with both intent and some capability. It is logistically easier to mount a cyber than a physical attack, there is more scope for easy innovation and there are many potential attack vectors.

Aviation is particularly vulnerable to cyber threats due to its reliance on a wide breadth of operational and safety-critical digital systems, often based on insecure legacy systems. Cyber attacks can impact safety, data privacy and protection, operational resilience, financial transactions, reputation and physical security. Increasing digitalisation has created new vulnerabilities.

The ability for cyber threat actors to attack victims remotely, often over long periods with low risk of identification or sanction, yet with lucrative outcomes means that it is an attractive approach. This is very different in nature from physical security attacks where deterrence is regarded as a key aspect of defence. It requires a different approach to assessing and managing the risks.

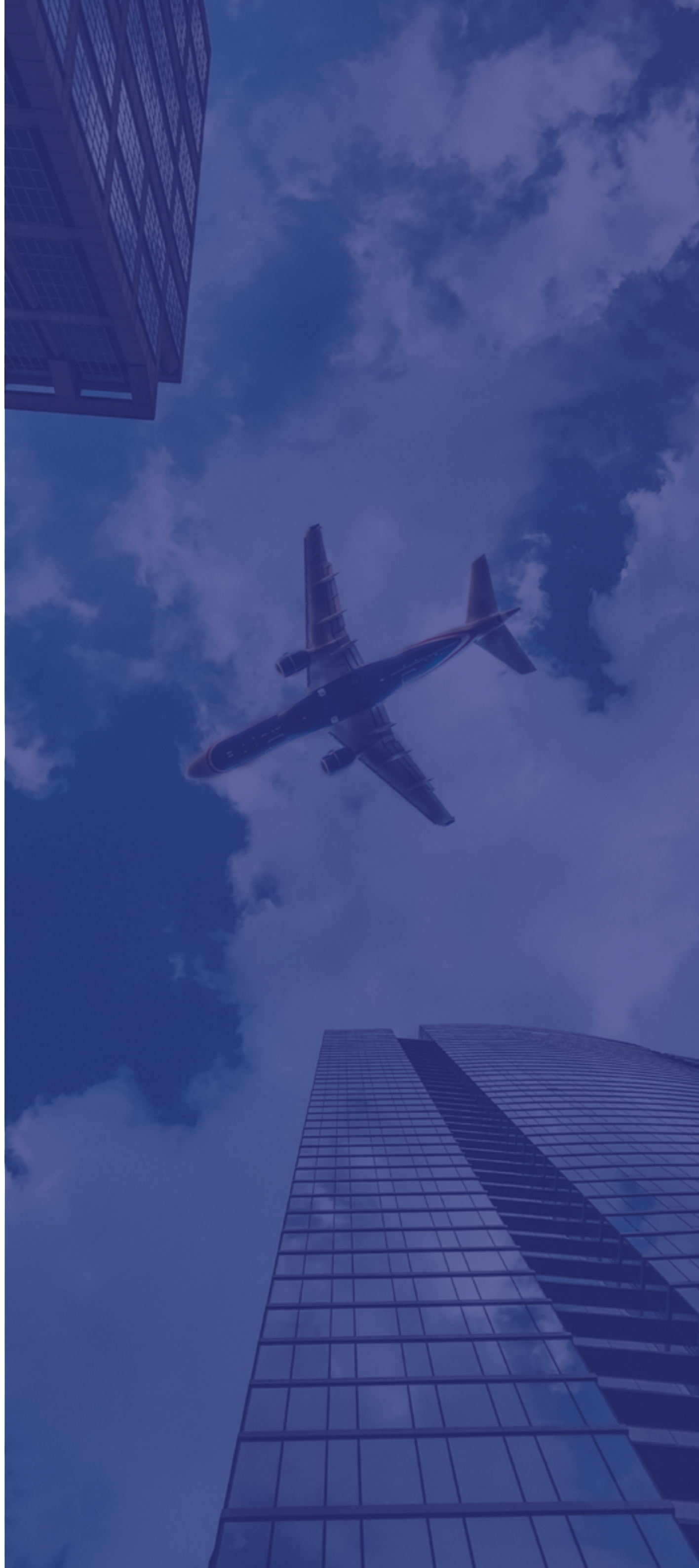
The rapid pace of change in technology and digitalisation coupled with the constant challenge of managing emerging vulnerabilities and exploits means that cyber threats are more dynamic than physical threats. Cyber threats carry greater uncertainty and as new vulnerabilities are identified every day, risk assessments go out of date more quickly than physical security threat assessments.

2.3 The difficulty of managing hybrid threats due to silos

Physical, facility and cyber security teams often have different reporting lines, objectives and incentives. Corporate security teams rarely have responsibility for cyber. IT security teams may not have responsibility for aviation operational technology. While there are examples of collaboration between the different security disciplines, this is often quite rudimentary and some way from the holistic approach needed to manage and mitigate the threats effectively and efficiently.

Cyber security threats, emerging from the ubiquitous interconnectivity enabled by digitalisation, require a corresponding collaborative security response. This interconnectivity cuts across the historical approaches to aviation security, particularly organisational structures and the way different specialisms work together.

To complicate matters further, security risk managers now need to consider the possibility of cyber attacks being used as a means of targeting physical assets, and vice versa. Similarly, there is increased complexity of unintended impacts from risk mitigations and contingencies in both the physical and cyber domains that needs to be considered.



2.4 People risk is bigger than many realise

Nation states, extremists and organised crime groups have long known and exploited the benefits insiders can bring to advancing terrorist plots and criminal endeavours. With the sector's increased connectivity and more aviation-related activities moving off-airport, or becoming virtual, the 'recruitment' pool available to bad actors continues to expand. Insider threats are not limited to acts of terrorism and organised crime though. Growing concerns over climate change and other environmental issues may influence insiders to take direct action against sector assets and operations, or facilitate others to do so.

Making use of an insider in the physical or cyber realm or both may make it easier for a bad actor to deploy a new form of attack. It is made even easier if inadequate controls to monitor user activity allow a perpetrator to remain undetected for a long period of time. Cyber attacks may have the added advantage of being logistically easier for an insider to mount than physical attacks and often have a lower risk of attack details being compromised due to the minimal involvement of people other than the attackers.

Organisations often place more focus on hardening physical security than investing in measures to mitigate insider threats, and this creates exploitable gaps in their security defences. The addition of cyber and hybrid risk surfaces compound this exposure.

3. The structural challenges

3.1 The need for a multi-disciplinary approach

Preventing acts of unlawful interference to civil aviation requires a multi-disciplinary approach

With the expanded range of threat vectors available to malicious actors, the task of preventing acts of unlawful interference has become more complex, requiring a multi-disciplinary approach. This need for a multi-disciplinary approach applies to when and how activities relating to threat modelling, risk assessment, risk treatment and overall risk management are performed. In some instances, this may consist of relatively straightforward adaptation or extension of existing activities, such as those relating to governance. In other instances, more complex activities are involved that require careful consideration of the organisational changes that are required.

Governance is often an obstacle to multi-disciplinary working

In an ideal scenario, a new fully integrated way of working would be put in place. This is unlikely to be supported by executive management given the likely scale of organisational change required and differences in standards and ways of working. However, the existing governance, risk and compliance (GRC) mechanisms tend to be an obstacle to multi-disciplinary working.

All organisations have GRC mechanisms at corporate level, which control the delivery of corporate objectives through departmental objectives, budgets and risk management. For each department (and within them, each individual), objectives are created as a subset of the corporate objectives, often with inadequate consideration of interdependencies or collaboration. Without common governance, individuals' job descriptions, objectives and deadlines are set separately, cascading from the objectives of the team they belong to. In organisations where that is the case, collaboration is often not empowered; any collaboration that is not in the business plan is unfunded and usually cannot be maintained consistently.

Some organisations have tried to address this with matrix management. This can be an effective approach but has its own challenges and may need to be introduced across an entire organisation rather than just to the areas responsible for security.

3.2 Weaknesses in the approach to security management

Current security management approaches tend to suffer from three major shortcomings.

The compliance habit

The aviation sector is characterised by a compliance-based focus toward aviation security, which often hinders an agile response to the rapidly emerging cybersecurity threat.

Initiatives like the Security Management System (SeMS) Framework[4] encourage operators to look beyond compliance, but SeMS is optional, and the concept has not yet completely overcome the compliance focus. Recent indications from the UK CAA suggest that the SeMS will be made mandatory for aviation security[5] and the introduction of a performance-based oversight processes for managing aviation cybersecurity via the ASSURE[6] scheme provides further indication of intent. The roll-out of the ASSURE scheme will remain a challenge for UK operators until they improve their overall management of aviation security and adopt a risk-focused approach.

Shortcomings in risk assessment techniques

The aviation industry has years of expertise in safety risk assessment, where risks can be modelled and managed with considerable accuracy thanks to the consistent properties of components and the volume of available data and statistical analysis of safety factors.

For aviation security risks, there is little relevant quantified history on which to base analysis. Indeed, a single event may give rise to a new regulation virtually worldwide, as seen with the introduction of limits on liquid, aerosol and gel volumes permitted in carry-on luggage, in response to the Al-Qaeda liquid bomb plot in August 2006. Attackers and attacks are by their nature unpredictable (what, when, where), so risks are difficult to quantify and are dynamic and unpredictable in nature. In security, risk assessments and ad-hoc threat assessments are therefore more reliant on expert judgement than calculation.

Nor can aviation risks be managed simply by using the same management system as enterprise risk: not only does the corporate system rely on being able to quantify risks, but also assessing the risk of loss of life in financial terms is fraught with reputational and legal risk.

The result is a limited understanding of security risks at corporate level. While this more often gives rise to inappropriate acceptance of risks, it sometimes gives rise to additional and unnecessary direct or opportunity costs characterised by the phrase "abundance of caution".

A new challenge: managing continuity of service

Historically, the continuity of service has not been regulated. Perhaps it was controlled to an acceptable level via aviation security controls, so no specific regulation was needed. Digitalisation has changed this, so cyber risks can now have an impact on continuity of service. The need for greater control of this effect has led to the EU Network & Information Systems (NIS) Directive and UK NIS regulation. This means that the risk management system for aviation compliance now needs to consider service continuity for operators that are in-scope of NIS regulations (i.e. Operators of Essential Services (OES)).

3.3 The means of achieving and maintaining trust needs to adapt

The compelling need for trustworthy aviation systems

The globe-spanning nature of aviation requires dependencies between a multitude of different parties to provide a safe and reliable service. As such, it is reliant upon the trust between the various parties that has been built by years of demonstrated performance and reinforced by rigorous assurance practices. It is not enough to rely on inspections and tests of the components of a system or the whole system. Assurance is based on evidence that the system is trustworthy – that it and all its components meet specific requirements by design so that the capabilities and services it delivers can be relied upon.

Security assurance is not limited to security considerations: trustworthiness requirements can include safety, security, reliability, dependability, performance and resilience under a wide range of potential adversity in the form of disruptions, hazards, and threats.

With the continually changing threat of cyber, physical and hybrid attacks, the means of ensuring aviation systems are trustworthy (including operators and their machine, physical and human components and passenger interactions) has never been more important. Cyber threats can undermine the established trusts in the technology even as we become ever more reliant on it. It also presents new threats to people, both through the manipulation of unsuspecting technology users and through the grooming of insider threat actors. Hence, the means for ensuring trustworthiness of systems is a growing concern.

Achieving trust in third parties is key

The high levels of outsourcing and interdependencies between aviation organisations leaves the sector particularly exposed to third-party cyber risks. The need and means for achieving assurance of aviation security service suppliers is well established but pre-dates the emergence of cyber risks. These risks can include the security of confidential data that they hold and the integrity and availability of any staff and security equipment that they use to deliver a service.

Establishing and maintaining the trustworthiness of supplied aviation security equipment is another, potentially novel, aspect of managing aviation security risks. While certain screening equipment has to be certified for performance, this does not extend to the cybersecurity of the equipment itself. Cybersecurity controls can either be ‘built-in’ by the supplier or ‘built-on’ by the user. An appreciation of what adequate ‘built-in’ security is, how the supplier provides assurance of this and the implications of managing any deficiencies in built-in security is key.

An organisation’s procurement and IT security teams may have established a process for cybersecurity assurance of third parties, but this is typically focused on IT related services and may not effectively identify and manage broader aviation security risks.

> “A series of high-profile, very damaging attacks on companies has demonstrated that attackers have both the intent and ability to exploit vulnerabilities in third-party security. This trend is real and growing. So, the need to act is clear.”
>
> **Supply chain security guidance – UK’s National Cyber Security Centre**

4. Rising to the challenge: the changes that matter

Introducing change can be hard, but with so many methodologies, techniques and tools, the obvious solution of establishing a common process and terminology is unrealistic. A more useful approach is to provide an outcome-focused overarching framework that can 'host' all specialisms and their ways of working. Within that framework there are several key touchpoints, where collaboration is supported by what might be called common interfaces or APIs.

This does not require a major restructure or re-skilling, and is achievable in small steps at a pace the organisation can sustain. It has three main components:

- Create the conditions to facilitate collaboration
- Drive the evolution of collaborative security methods
- Redouble efforts to manage the people risks

While operators will most likely need to acquire or grow certain capabilities, adopt new technologies and introduce new practices, the required disciplines and management systems already exist to a large extent within organisations. Rearchitecting the existing elements that make up the governance, risk and security systems (people, processes and technology) to address the collaboration challenge successfully not only provides a more optimal way for managing security risks, but also supports organisations in realising the opportunities that digitalisation offers.

There is a parallel with an electric car conceived and designed from the ground up, as opposed to a petrol car whose engine and fuel tank have been replaced by electric motor and battery but is otherwise unchanged. Simply replacing certain processes rather than looking at the whole will not give the most streamlined interfaces or the smoothest collaboration.

> "Providing satisfactory security controls in a computer system is… a system design problem. A combination of software, communications, physical, personnel and administrative procedural safeguards is required for comprehensive security… software safeguards alone are not sufficient."
>
> **NIST SP 800-53, Rev. 5 quoting**
>
> **The Ware Report: Security as a Design Problem – Defence Science Board Task Force on Computer Security, 1970**

4.1 Recommendation 1: Create the conditions to facilitate collaboration

Governance of collaboration

As noted earlier, GRC mechanisms at corporate level control the delivery of corporate objectives through departmental objectives, budgets and risk management. To create an environment in which security collaboration thrives, an organisation should ensure its corporate objectives include security, either as an explicit objective in its own right or as a component of other corporate objectives. This is not a new concept. Organisations have management systems and governance frameworks for control of the business, and these can be extended with compromising them, to provide the common language for security risk management.

The organisation should also adjust corporate governance to specify "collaboration objectives" – creating, monitoring, and funding departmental objectives that mandate collaboration across departments to facilitate their shared responsibility for delivering corporate security objectives.

To deliver the collaboration objectives, the different security departments might form a Security Threats and Risks (STAR) group to collaborate on managing security threats and risks, bringing together security professionals and business representatives from the organisation and its partners and suppliers

In support of that, the enterprise risk management mechanism should engage with security department managers to monitor risks to delivery of departmental and therefore corporate security objectives. Individual security risks managed by the STAR group or the individual security departments should not figure in the enterprise risk management process unless they affect the corporate objectives.

Governance of security

A risk committee, such as the STAR group, is the cornerstone of security governance. Its remit is to identify, assess and manage security risks on behalf of the business in accordance with corporate objectives, which include compliance with the relevant aviation and cyber security regulations.

To supplement compliance, the organisation should evolve a risk-focused approach to aviation and cyber security, much as it has done for financial and other corporate risks.

The UK Civil Aviation Authority (CAA) has provided the tools for this, the Framework for an Aviation Security Management System[7], the Cyber Security Oversight Process for Aviation[8] and the Cyber Assessment Framework for Aviation (CAF)[9]. The CAA determines the effectiveness of an organisation's security risk management by assessing its SeMS against the Framework and its cyber security effectiveness through an accredited third-party cyber security audit scheme "ASSURE" which is in effect a risk-based approach.

The SeMS Framework provides a comprehensive governance structure and supporting elements for:

- A common governance over the specialist areas
- Tasking and enabling specialists to collaborate in management and escalation of the major threats and risks within the organisation's risk tolerance limits
- A systems-thinking approach to end-to-end security management
- Robust supplier management of the component systems/subsystems
- Business justification of security budgets, including the opportunity costs of over-cautious security

The Framework is not just for physical security – or indeed, it is not just for aviation. It is equally relevant to retail, maritime or any organisation, large or small. It is highly adaptable, and is readily applicable to cyber security.

Like the example of good electric car design, the elements that make up the SeMS are largely the same as 'classic' security but the resulting package is superior and much more appealing.

> SeMS provides a formalised, risk-driven framework for integrating security into the daily operations and culture of an Entity. The SeMS enables an Entity to identify and address security risks, threats, gaps and weaknesses in a consistent and proactive way.
>
> **SeMS Framework (Introduction) – UK Civil Aviation Authority**

4.2 Recommendation 2: Drive the evolution of collaborative security methods

Governance changes remove the obstacles, but further work is required to establish collaboration between the security teams.

The Security Threats and Risks (STAR) group should be charged with this work, using the Security Management System (SeMS) Framework as the template. The simplicity of the SeMS Framework makes it relevant to every team's approach to managing threats and risks regardless of whether they are physical, cyber or hybrid.

Thoughtful application of the SeMS Framework will lead to common, overarching management systems aligned across the disciplines. 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.

Areas include:

- Risk identification and assessment of both ad-hoc events and persistent risks – ensuring that all risk types (e.g. legal, regulatory, sustainability, financial, continuity, privacy etc.) are considered, that signals are not missed, that best practices are shared, that knowledge is pooled, and that trained assessors are in place for instant assessment of ad-hoc events
- Incident management – managing ad-hoc events to a secure conclusion
- Risk management – ensuring approaches work together efficiently and effectively, that non-regulated security threats such as fraud are also considered, and that risk treatments are holistically optimised for an organisation
- Enterprise security impacts – monitoring the achievement of security objectives and any aggregation of risks to identify security risks that need to be escalated to top management, and enterprise risk effects that need to be escalated to the enterprise risk team
- Third party selection and contracting – involving all relevant stakeholders to ensure all risk types, including cyber security risks that may have a broader aviation security effect, are considered holistically for the full lifecycle of the engagement with the third party, and are an appropriately weighted factor in supplier selection
- Third party assurance – establishing as part of the contracting process a regime of performance reporting, monitoring and/or assurance audits proportionate to the associated risk
- Compliance, monitoring and reporting – aligning and maturing management systems, streamlining activities, and tailoring metrics to the current security landscape
- Confidential reporting – enabling and encouraging staff to report security concerns that have no other means of capture
- Insider threat management – ensuring complete coverage of all staff, streamlining programmes and ensuring that signals are not missed
- Resourcing – competency management plans, staff development and recruitment provide the mixed skill sets needed for addressing aviation cyber security

Having developed these processes into the SeMS, the STAR group will use the SeMS to provide the organisation's collaborative security management 'service'. The STAR group is itself a collaborative team made up of managers and specialists from each of the security teams and from the business. In addition to a standing agenda to monitor and review security risks, the group or subsets of the group will be the resource for each of the processes in the SeMS, calling on further specialists from their own teams as needed.

A clear picture of the major threats and risks, maintained by an agile STAR group, provides corporate assurance of security and prevents an abundance of caution when responding to incidents and new business opportunities alike.

4.3 Recommendation 3: Redouble efforts to manage people risk (insider threat and competence)

Security protects a “system of interest” from malicious or accidental interference with the correct functioning of the system, which in this context is aviation and aviation operators: each operator within the sector is a system made up of people, processes and technology. Despite increasing automation being critical to future operations, people will always be vital components of the security system because of their intuition and initiative. Their adaptability to unexpected circumstances makes them a vital security resource but equally means that they can be exploited by bad actors.

As highlighted in this paper, people risk is bigger than most people realise and there are concerns about the growing dependence on IT systems, which is driving a potential increase in insider activity. With such a diverse and dynamic threat landscape, defending against insider threats must become a priority task for organisations. There is a need for them to redouble their efforts to manage people risk by continually assuring, and where necessary, strengthening their insider threat defences to help them stay ahead of new and emerging risks. This level of proactivity together with assurance oversight must extend to their supply chain, to ensure there are no weak links. Terrorists and other bad actors will invariably seek the path of least resistance. Therefore, a whole system approach works best when it comes to managing people risk.

In times of uncertainty, it is easy for organisations to become distracted and lose sight of their actual risk picture, but insider threats can become ticking time bombs if not identified and managed, as historic cases reveal. Challenging current assumptions and processes insofar as people risk should become a habit, and there is a wealth of relevant guidance material on managing people risk available from the UK’s Centre for the Protection of National Infrastructure and the National Cyber Security Centre.

The cultural elements impacting people risk are worthy of specific mention: leadership behaviours, commercial priorities and targets, together with how staff are treated and rewarded all play a key role in moulding an organisation’s culture. The need for leaders to act transparently and with integrity, and the fair treatment and reward of the workforce, will reduce the risk of a toxic culture, and all the risks that brings, from emerging. Another benefit of adopting the SeMS Framework is the guidance it gives on demonstrating management commitment, clear accountability and good communications.

> People are an organisation’s biggest asset, however in some cases they can also pose an insider risk. As organisations implement increasingly sophisticated physical and cyber security measures to protect their assets from external threats, the recruitment of insiders becomes a more attractive option for those attempting to gain access.
>
> **Reducing insider risk – Centre for the Protection of National Infrastructure**

5. Now is the time

The potential damage to aviation of cyber attacks is far greater than those that have occurred to date. The cyber attack, and particularly the hybrid cyber-physical attack, is probably aviation's most threatening Gray Rhino: it is charging towards us. It may look distant but it is there and it is getting closer.

In the Cyber Security Oversight Process for Aviation (CAP1753) the UK Civil Aviation Authority states its vision for Cyber Security Oversight.

"To have a proportionate and effective approach to cyber security oversight that enables aviation to manage their cyber security risks without compromising aviation safety, security or resilience..."

Every operator should adopt this vision to have a proportionate and effective approach to cyber security, flying in formation with its physical counterpart.

Aviation organisations need to evolve their current approaches to safety and security to adapt to the rapidly evolving threat landscape that the sector faces in this time of rapid digitalisation. By adopting a collaborative and proactive risk-based approach, such as the one discussed in this whitepaper, they will be able to keep pace with cyber threats and effectively exploit the benefits of digitalisation. The frameworks and methodologies for achieving this are already available, what is also needed is an openness to collaboration and change.

> The leaders best equipped to outsmart a Gray Rhino have access to warning signals and pay attention when the alarm sounds. They know what to do to get out of the way, or, at least, they blunder through enough trials and errors to mitigate the rhino's charge.
>
> **The Gray Rhino – Michele Wucker**

6. Glossary

CAA	Civil Aviation Authority
CAF	Cyber Assessment Framework
CPNI	Centre for the Protection of National Infrastructure
GRC	Governance, Risk and Compliance
IT	Information Technology
NCSC	National Cyber Security Centre
NHS	National Health Service
NIS	Network and Information Systems
OES	Operators of Essential Services
SeMS	Security Management System
STAR	Security Threats and Risks

7. References

1. Defined by the International Civil Aviation Organization (ICAO) as “protecting civil aviation against acts of unlawful interference”. The European Civil Aviation Conference (ECAC) expands this as “securing airports, aircraft, passengers, cabin baggage, hold baggage, cargo and mail, in-flight supplies and airport supplies. Provisions on in-flight security, ATM and cyber security and the management of threats and hijackings…”. The UK Civil Aviation Authority (CAA) and others point out the importance to aviation security of third party suppliers and the entire supply-chain.

2. The 9/11 Commission Report Chapter 11, 9/11 Commission (2004)
https://govinfo.library.unt.edu/911/report/911Report.pdf

3. The Gray Rhino, Michele Wucker - St Martin’s Press (2016)

4. CAP1223: Framework for an Aviation Security Management System (SeMS), UK Civil Aviation Authority
https://publicapps.caa.co.uk/modalapplication.aspx?appid=11&catid=1&id=6543&mode=detail&pagetype=65

5. “Why Performance Based Oversight, SeMS and professionalisation of training are imperative for the aviation sector”, International Airport Review, 19th November 2020, https://www.internationalairportreview.com/article/144497/performance-based-oversight-sems-imperative-aviation/

6. CAP1753: CAA Cyber Security Oversight Process for Aviation UK, Civil Aviation Authority
https://publicapps.caa.co.uk/modalapplication.aspx?appid=11&catid=1&id=9242&mode=detail&pagetype=65

7. CAP 1223: Framework for an Aviation Security Management System, UK Civil Aviation Authority

8. CAP 1753: The Cyber Security Oversight Process for Aviation, UK Civil Aviation Authority

9. Cyber Assessment Framework (CAF), Civil Aviation Authority
https://www.caa.co.uk/Commercial-industry/Cyber-security-oversight/Cyber-security-compliance/

10. Reducing Insider Risk, Centre for the Protection of National Infrastructure
https://www.cpni.gov.uk/reducing-insider-risk

11. People-centred Security, National Cyber Security Centre https://www.ncsc.gov.uk/section/advice-guidance/all-topics?topics=People-centred%20security&sort=date%2Bdesc

3DAssurance

3DAssurance specialises in management systems for providing assurance that corporate risks are fully managed with ready-made or tailored solutions to the management 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. We ensure the sustainability of our solutions by embedding them with mentoring and training in the principles and practices, supporting continuous improvement activities where appropriate.

www.3dassurance.com

NCC Group

NCC Group exists to make the world safer and more secure. As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 clients worldwide to protect their most critical assets from the ever-changing threat landscape. With the company's knowledge, experience and global footprint, it is best placed to help businesses identify, assess, mitigate and respond to the evolving cyber risks they face. To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists. With over 1,800 colleagues in 12 countries, NCC Group has a significant market presence in North America, continental Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia and Singapore

www.nccgroup.com