Working Together for a Cyber Resilient Future in Aviation

Webinar – 24th July 2024

Questions & Answers

Audience Question	Panellist Answer
Has anyone else investigated applying Systems Theoretic Process Analysis (STPA) to Cybersecurity? I know here in the UK that the NCSC was pushing this to help create meaningful risk appetites in complex systems.	The UK CAA has looked at STPA as part of a proposal to identify risk assessment methodologies, however we do not use this method ourselves. We use a standard 5X5 risk approach.
Does the police in the UK offer cybersecurity training for employees of critical infrastructure such as airports or fuel depots?	The Police provide CNI training and support through the National Protective Security Authority (NPSA) to critical national infrastructure (CNI) providers. This is primarily coordinated through the NPSA and the National Cyber Security Centre (NCSC). The NPSA works closely with businesses and organisations within the CNI sectors to identify risks and vulnerabilities, offering advice to reduce these risks. This collaboration includes the Police and other security specialists to ensure comprehensive protection of essential services (National Protective Security Authority) (ProtectUK). The NCSC, as part of its mandate, provides technical advice and support to CNI operators to enhance their cybersecurity measures. This includes developing and sharing cybersecurity principles and providing direct support during incidents. The NCSC also acts as a liaison between UK organisations and EU Member States regarding cybersecurity issues (GOV.UK).

	These efforts are part of a broader national strategy to safeguard critical infrastructure from various threats, including cyber-attacks, and to ensure resilience and continuity of essential services (GOV.UK).
What are the seven pillars?	Covered in session 2 - The pillars are from the ICAO Cybersecurity Strategy Aviation Cybersecurity Strategy (icao.int)
Can someone please differentiate ANC and ATB?	Covered in Session 2 – Air Navigation Commission (Safety) Air Transport Bureau (Security). https://www.icao.int/Security/USAP/Pages/The-Critical-Elements.aspx
32 priority action? 51 tasks? If it can be elaborated a bit more	ICAO document that drives the work (Actions/Tasks) of the Cybersecurity Panel. Cybersecurity Action Plan (icao.int)
Can you comment on the recent CrowdStrike incident, whether it could have been prevented or any action the aviation cybersecurity community should take / implement / learn?	CrowdStrike has now issued its initial incident report including the following summary: • The update involved a 'rapid sensor' content update, which contained an undetected error. • The sensor release process begins with automated testing, which include, unit testing, integration testing, performance testing and stress testing. • This culminates in a staged sensor rollout process, that internally at CrowdStrike, followed by early adopters, before being made available to customers. • Customers can then select which parts of their fleet should install the latest sensor release, according to different release version settings. • Friday's update was not triggered by Sensor Content. Two additional templates were deployed but included a bug Content Validator, meaning that one of the two Template Instances passed validation despite containing problematic content data. • When received by the sensor and loaded into the Content Interpreter, problematic content in Channel File 291 resulted in an out-of-bounds memory read triggering an exception and causing the Windows operating system crash (BSOD). In addition to this preliminary Post Incident Review, CrowdStrike is committed to publicly releasing the full Root Cause Analysis once the investigation is complete. *Could it have been prevented?* Yes, the context update could have been compiled without the unexpected error, the actions identified by CrowdStrike should detect such issues in future.

	Any action the aviation cybersecurity community should take/implement/learn? Customers using CrowdStrike should understand which parts of their fleet should install the latest sensor release and what the appropriate version release settings should be. I.e. one version older ('N-1') or two versions older ('N-2') through Sensor Update Policies.
How does the CAA ensure that organisations have a cyber resilient system when doing oversight? What do we check to satisfy ourselves that the organisation is cyber resilient?	The UK CAA continues to work with organisations across aviation to ensure good cybersecurity. Most organisations have completed initial oversight with the UK CAA and received a Certificate of Compliance. Through our cybersecurity oversight, we work closely with industry cyber contacts to ensure a robust approach to cyber, including effective categorisation of critical systems and ensuring that incident and resilience plans are robust and in place. It is imperative that organisations understand and map their supply chains to ensure the criticality of their suppliers and the impacts they can have on critical aviation systems. Resources include: • NCSC Mapping guidance: Mapping your supply chain - NCSC.GOV.UK • NCSC communication around assurance: How to assess and gain confidence in your supply chain... - NCSC.GOV.UK • Follow Government Supplier Assurance framework: Government supplier assurance framework - GOV.UK (www.gov.uk)
How effective is it having a sectoral CERT for the aviation industry?	In Singapore, we developed a joint aviation sectoral Security Operations Centre (SOC) which tailored responses specific to threats unique to aviation. This aims to enhance sectoral awareness, provide early warning detection, and enable faster sectoral response. This allows closer coordination among key aviation stakeholders in Singapore including airlines, airports, and regulatory authorities. Separately, we collaborate closely with the Singapore Cyber Emergency Response Team (CSA SingCERT) and the Government Technology Agency (GovTech) to respond to cybersecurity incidents.

How does the CAA organise oversight activities? On-site assigned AvSec managers are not cyber–Subject Matter Experts and need to coordinate with the entity`s cybersecurity experts which will likely not be on site and may be working in different time zones.	The UK CAA requires an organisation to have defined roles, which include the Cybersecurity Responsible Manager (CSRM). The CSRM acts as the point of contact and is the key contact when arranging oversight activities. This is defined in CAP1753. As part of our evolving ongoing oversight approach, our Cybersecurity Oversight specialists ensure that entity communications are distributed to designated Cybersecurity Responsible Managers (CSRMs) and Security Managers to ensure awareness and collaboration. Comments regarding cybersecurity experts in different time zones may be particular to individual organisations, and the UK CAA, as a regulator, is not able to comment on the makeup of support resources.
Is the SOC mandatory for the establishment of the Cybersecurity framework in CNS ATM area?	SOC is understood to be an acronym for a Security Operations Centre, and while the CAF does not mandate this, it is a highly recommended security control provision.
Can you comment on how the SeMS model would operate with existing cybersecurity requirements?	The SeMS framework is separate from the UK CAA's Cybersecurity Oversight approach. However, some areas of control may overlap and provide compliance with the relevant requirements across the SeMS framework, the CAF, and requirements set out by the Single Consolidated Direction (chapter 13).
What exactly do you mean by "Security a horizontal rule"?	A horizontal rule is a term for a regulatory framework implemented across traditionally separate areas of regulation, in this case, existing safety and security regulations.
As EU and UK authorities look to regulate Ground Handling, do you envisage Ground Handlers coming into your cyber regulation/oversight model?	The UK CAA does not apply cybersecurity regulation to the wider supply chain. Work is underway from a national perspective to consider regulating the supply chain, this does not currently have a timeline.

I believe you said UK Regulation is advised not enforced on suppliers, is this likely to change in the future?	Currently, the UK CAA does not apply cybersecurity regulation to the wider supply chain. Work is underway from a national perspective to consider regulating the supply chain, this does not currently have a timeline. It is imperative that organisations understand and map their supply chains to ensure the criticality of their suppliers and the impacts they can have on critical aviation systems. Resources include: • NCSC Mapping guidance: Mapping your supply chain - NCSC.GOV.UK • NCSC communication around assurance: How to assess and gain confidence in your supply chain... - NCSC.GOV.UK • Follow Government Supplier Assurance framework: Government supplier assurance framework - GOV.UK (www.gov.uk)
Why does ICAO doc 9839 QMS for ais mention integration for QMS and SMS but nothing is related to security? Is it any specific guidance how to integrate systems in ICAO, that means QMS, SMS AND SeMS or ISMS?	The UK CAA is considering integrating existing management system approaches into the Information Security Management Systems (ISMS) approach and will form future guidance.
What is the relationship between aviation security and CS in practice?	In the UK CAA, the Cybersecurity team is part of AvSec, and we work together on our cyber oversight programme.
How does the UK CAA foster collaboration with other States particularly, African States, in the field of cyber security?	The UK CAA plays an active role in ICAO through the Trust Framework and Cybersecurity Panels. It also participates in global capacity-building work with the likes of ECAC and through its advisory and training arm, CAA International.

What is the duration of the report to the authorities if there is any cybersecurity attack?	Under the NIS 2018 requirements from a national perspective there is a reporting requirement within 72 hours. For other directed entities, incident reporting to the UK CAA is not currently mandated. However, we invite entities to provide details of any events and incidents they experience, even if they do not have a direct safety impact. Reporting such events to the UK CAA will help ensure a better understanding of the threats and risks posed to industry and enable the UK CAA to provide timely advice for other organisations that may experience similar events, contributing to improving the overall security posture of UK aviation.
Coming from a developing country, Papua New Guinea, we have yet to establish a regulatory framework for aviation cybersecurity. What is your advice on where we should start?	In the first instance, developing nations can contact ICAO directly through their regional network for support and guidance. Additional advisory and training services are also available via CAAi.
Most of our aviation systems are isolated and use Linux as an OS, providing high-level security. Do we need to focus on educating employees in programming or SE to be experienced in how to attack security issues from hackers?	The UK CAA does not advocate tailored advice on approaches for specific technologies or operating systems. Entities are expected to decide on their technology stack and the required security to protect these services. In general, the UK CAA advises focusing on the basics, including ensuring a robust security update process is established, that employee cyber training is undertaken, and that an incident plan is in place and exercised.
The CASE 1A Checklist, which is used by US flag carriers to audit Part 145 MRO, already mandates the requirement to have a cybersecurity policy. Will there be any from CAAS or CAA UK?	145.A.200A Information security management system In addition to the management system referred to in point 145.A.200, the maintenance organisation shall establish, implement and maintain an information security management system in accordance with Implementing Regulation (EU) 2023/203 in order to ensure the proper management of information security risks that may impact aviation safety. *Regulation (EU) 2023/203 - Applicable from 22 February 2026*

How do you envisage small to medium operators achieving Cyber resilience when organisations such as the NHS, Banks and even the UK Government with all their resources cannot achieve this?	The UK CAA provides oversight to smaller organisations against a simplified version of the CAF known as Foundational Elements (based on Cyber Essentials) and is also developing an ISMS approach to cybersecurity that will be risk-based and proportionate. The UK CAA advises organisations with limited resources to focus on the basics, including ensuring a robust security update process is established, employee cyber training is undertaken, and an incident plan is in place and exercised.
A main concern regarding security within the supply chain (SC), particularly in light of the NIS2 directive, is ensuring its resilience and robustness against cyber threats. What's the CAA's view in this regard, and what processes can be adopted to ensure peace of mind (to some extent)?	The UK CAA does not apply cybersecurity regulation to the wider supply chain. Work is underway from a national perspective to consider regulating the supply chain, but there is no timeline currently. Organisations must understand and map their supply chains to ensure the criticality of their suppliers and the impacts they can have on critical aviation systems. Resources include:: • NCSC Mapping guidance: Mapping your supply chain - NCSC.GOV.UK • NCSC communication around assurance: How to assess and gain confidence in your supply chain... - NCSC.GOV.UK • Follow Government Supplier Assurance framework: Government supplier assurance framework - GOV.UK (www.gov.uk).
From a cost-benefit perspective regarding cyber threat detection within the aviation sector, is it recommended to set up an SoC (Security Operation Centre) for a specific organisation or an industry-based SoC that involves airlines, regulators, and airports?	SOC is understood to be an acronym for a Security Operations Centre. While the CAF does not mandate this, it is a highly recommended security control provision.
Is there a proportional approach to regulation in the UK for very small organisations?	The UK CAA provide oversight to smaller organisations against a simplified version of the CAF known as Foundational Elements (based on Cyber Essentials) and is also developing an ISMS approach to cybersecurity that will be risk-based and proportionate.

To ensure cybersecurity resilience in the future, we need training. Has CAA Singapore established a training structure/programme?	We are collaborating with partners, such as UK CAAi, to develop appropriate training programmes in cybersecurity and resilience. This webinar is one such initiative, and we hope you have some takeaways from this sharing.
Will CAAS & CAA consider enforcing ISO/IEC27001:2022 to secure aviation ISMS?	CAAS may incorporate or recommend ISO/IEC 27001 as part of their broader information security or cybersecurity frameworks, especially for organisations dealing with sensitive aviation data. However, adopting specific standards like ISO/IEC 27001:2022 can depend on national regulations, the organisation's specific needs, and the overall regulatory strategy for aviation security. From a UK CAA perspective, we are unlikely to request specific accreditation, such as ISO, as part of implementing the future ISMS approach in the UK.
How does the Civil Aviation Authority plan to address the threat of cyber-attacks on systems, particularly in terms of securing both ground infrastructure and in-flight systems? Also, what protocols or technologies are being implemented to ensure the resilience of critical aviation infrastructure?	The UK CAA is not responsible for addressing the threat of cyber-attacks on specific systems but is responsible for working with entities to ensure that they are taking the necessary steps to protect their services. It can offer guidance and advice on how to approach this. That advice will not be tailored to specific technologies; entities are expected to decide on their technology stack and the required security to protect these services. We encourage entities to work closely with NCSC, joining aviation (or sector-specific) groups, subscribing to their early warning service, reading and acting on assessment digest communications, etc. The UK CAA generally advises focusing on the basics, including ensuring a robust security update process is established, that employee cyber training is undertaken, and that an incident plan is in place and exercised. National Aviation Authorities and relevant organisations are taking comprehensive steps to address the threat of cyber-attacks on both ground infrastructure and in-flight systems, E.g. collaborating with ICAO on aligning Aviation Cybersecurity standards and best practices, implement regulatory compliance checks, conduct cybersecurity training and exercises, perform continuous monitoring, detection and patch management, conduct risk assessments, review and implement security by design to strengthen the overall resilience of the critical aviation infrastructure.

Do you think cyber threats to the aviation sector are different from those to other sectors? If so, what do you think are the key cyber threats to the aviation sector?	The UK CAA considers that threats to the aviation sector are broadly similar to the threats that are facing other Critical National Infrastructure (CNI) sectors, but that aviation, given its profile and the visible nature of any potential disruption, means that it is a very attractive sector for bad actors to effect disruption. We encourage entities to work closely with NCSC, joining aviation (or sector-specific) groups, subscribing to their early warning service, reading and acting on assessment digest communications, etc. Unlike many other sectors where cybersecurity primarily focuses on protecting data and systems, in aviation, cybersecurity also intersects with safety and physical security. Cyber incidents can directly impact flight safety and airport security, making it crucial to address these issues holistically. Some common cyber threats are aircraft system hacking on flight control systems, avionics, attacks on air traffic communication interference, attacks on drones and unmanned aircraft systems (UAS) etc.
Are there any security considerations in the use/adoption of AI in airport operations and processes?	The UK CAA would encourage entities to work closely with NCSC, joining aviation (or sector-specific) groups, subscribing to their early warning service, reading, and acting on assessment digest communications including those on future threats including Artificial Intelligence (AI). Security is being considered to ensure operational efficiency and safety when adopting AI in airport operations and processes. Since AI processes large volumes of sensitive data, due diligence should be exercised when adopting AI in airport operations and processes. National Aviation Authorities could work closely with aviation operators to ensure data protection regulations are being adhered to and cybersecurity measures are being implemented, e.g. Risk assessments, penetration testing, vulnerability scanning, etc.
What is the level of severity of a cybersecurity attack that requires authority attention?	The UK CAA say that under the NIS 2018 requirements from a national perspective, there is a reporting requirement within 72 hours. For other directed entities, incident reporting to the UK CAA is not currently mandated. However, we invite entities to provide details of any events and incidents they experience, even if they do not have a direct safety impact.

	Reporting such events to the UK CAA will help ensure a better understanding of the threats and risks posed to industry and enable the UK CAA to provide timely advice for other organisations that may experience similar events, contributing to improving the overall security posture of UK aviation. National Aviation Authorities can refer to national cyber threat alert level framework to determine the associated cyber threats, risk and impact assessments, trigger points and corresponding actions. The threat level is raised in the event of a cybersecurity incident causing significant damage or compromise to national security; this can be e.g. attacks on essential services like electricity, water, transportation, etc, large-scale attacks causing significant economic and safety disruptions, data breaches etc, or high-profile attacks which are highly sophisticated and well-coordinated etc. In such cases, CAAS will coordinate with our national cybersecurity, defence, and international agencies to share intelligence and coordinate responses.
GPS/GNSS jamming and spoofing are becoming more frequent. Especially over certain airspace. How can the NAAs help engage States with airspace that are more "prone" to such incidents?	To mitigate the effects of spoofing and jamming, National Aviation Authorities (NAAs) can conduct regular training for stakeholders (controllers, pilots, etc.) to raise their awareness of identifying potential threats, e.g., sharing the impacts of spoofing and jamming, etc. Separately, the stakeholders should also be familiar with the backup's procedures (e.g. land-based navigation aids, alternate GNSS etc), performing surveillance and reporting updates etc. In addition, NAAs should actively collaborate with ICAO and Industries to mitigate the efforts of jamming/spoofing. E.g. GNSS interference, tools for ANSPs to detect jamming/spoofing etc. The UK CAA has working groups, including cyber, Flight Ops and other capability areas, to consider the threats of GNSS jamming and spoofing and continually assess the potential for disruption, the impacts (possible and actual) and the potential mitigation and protection required for such threats, both from accidental/unintended and intentional acts. Collaboration and reporting are key to understanding these events' prevalence, circumstances, and impacts, so the CAA would encourage reporting both safety-related events through the Mandatory Occurrence Reporting (MOR) system and voluntarily reporting.

How can the aviation industry enhance its cybersecurity measures to protect against evolving cyber threats and ensure the safety and efficiency of air navigation services in the future?	The UK CAA is responsible for working with entities to ensure that they are taking the necessary steps to protect their services and can offer guidance and advice on how to approach this. We would encourage entities to engage with their assigned Cybersecurity Oversight Specialist for any specific questions. We encourage entities to work closely with NCSC, joining aviation (or sector-specific) groups, subscribing to their early warning service, reading, and acting on assessment digest communications, etc. In general, the UK CAA advises focusing on the basics, including ensuring a robust security update process is established, that employee cyber training is undertaken, and that an incident plan is in place and exercised. CAAS works closely with Critical Information Infrastructure to ensure that they meet the regulatory measures while working closely with the other aviation stakeholders to put baseline security controls in place to ensure that they have the appropriate measures and recovery processes to be resilient against cyber-attacks. Likewise, threat intelligence for the aviation sector and a close working relationship with the transport sector help to enhance the capabilities across the sectors.
Is AI taking a more active part in protecting systems. How is oversight of it managed?	AI is increasingly being considered and implemented in the Aviation Sector to enhance efficiency, safety, and customer experience. It is important to maintain a balance between operational and security considerations, and often enough, human operators are still integral to supporting and enhancing decision-making to ensure accountability in case of failures or incidents. In addition, to complement AI cybersecurity, there are regulatory oversight frameworks, continuous monitoring, etc, to ensure these technologies operate safely and effectively. The UK CAA is developing an AI strategy to set out guardrails. We would encourage entities to work closely with NCSC, joining aviation (or sector-specific) groups, subscribing to their early warning service, reading, and acting on assessment digest communications, including those on future threats, including Artificial Intelligence (AI).

Is ICAO considering implementing ISMS, like requiring SMS, QMS and recommending SeMS? Why is it not requiring ISO 27001 but is recommending ISO 9001?	ICAO leaves it to States to define their risk appetite to implement ISMS. ICAO recognises the need for wider collaboration beyond safety and security streams and is working with the respective expert panels and Standard Making Organisations (SMOs) to align the work and standards requirements. The future UK implementation of ISMS is not driven by ICAO, it is following the European approach to similar regulation through Part-IS. From a UK CAA perspective, we are unlikely to request specific accreditation such as ISO as part of the implementation of the future ISMS approach in the UK.
What would be the best approach to integrating Information Security processes into the existing aviation security management? What challenges would require arriving at a common ground on how risks are identified and reviewed? These are two different expertise. What would be the best approach, in the panel's opinion?	Integrating information security processes into existing aviation security management systems can be challenging due to each discipline's distinct expertise and focus areas. Information security (IS) primarily protects data and IT systems, while aviation security (AS) focuses on ensuring the safety and security of physical assets and operations. However, given the increasing interdependence of digital and physical security, effective integration, e.g. common risk assessment framework, alignment of policies, implementation of centralised security management system, etc., would be some of the approaches considered.
Does the Civil Aviation Authority provide any guidelines or resources for IT cybersecurity professionals interested in contributing to the development of more resilient cybersecurity systems within the aviation sector?	Cybersecurity professionals can leverage a wide range of resources provided by ICAO, NAAs, industry standards, and collaborative forums to understand more on the guidelines and best practices. However, only aviation professionals with specialised expertise in both aviation operations and cybersecurity are equipped to effectively contribute to the development of more resilient cybersecurity systems within the aviation sector.

Can you all share case studies of effective cybersecurity best practices and learning initiatives that proved useful to your staff or aviation operators and their customers?	There are several case studies that illustrate effective cybersecurity best practices and sharing initiatives within the aviation sector. These case studies highlight how such initiatives have been beneficial to staff, aviation operators, and their customers. Here are a few examples: • EU Cybersecurity Framework for Aviation (EASA) framework provides guidelines for managing and mitigating cybersecurity risks in aviation operations. • The International Air Transport Association (IATA)'s Aviation Cybersecurity Programme provides a platform for airlines and other aviation stakeholders to share cybersecurity best practices and threat intelligence. The Singapore Cybersecurity Act provides a legal framework for protecting critical information infrastructure, including those in the aviation sector.
How do you see ICAO Regional Offices learning from/engaging with the new ASEAN capacity-building work?	Collaboration is key, and ICAO Regional Offices can benefit from joint training programmes and resource sharing with ASEAN Singapore Cybersecurity Centre of Excellence. These efforts ensure that training aligns with both regional requirements and global standards, enhancing the overall quality and relevance of aviation training.
Does ICAO / CAAS recognise the different aspects of aviation CS regarding two key pillars: ground systems assurance and aircraft certification?	ICAO addresses the security of ground systems through frameworks and guidance that protect critical infrastructure such as airports and air traffic control systems. ICAO's Annex 17 and other documents provide standards to ensure these systems are secure from cyber threats. Similarly, CAAS enforces cybersecurity regulations for ground systems in Singapore, ensuring compliance with international standards and safeguarding essential IT infrastructure and operational technology. ICAO incorporates cybersecurity into certification standards for aircraft, focusing on securing avionics and onboard systems against cyber threats. These standards are designed to ensure that aircraft systems meet rigorous security requirements. CAAS aligns with these global standards, integrating cybersecurity into the aircraft certification process and maintaining oversight throughout the aircraft's operational life to ensure ongoing compliance.

How does cyber resilience support digital transformation?	Singapore is actively leveraging relevant laws and regulations and embedment of resiliency into our cybersecurity strategies e.g. protection of critical data, compliance with regulatory standards, continuous monitoring etc to bolster our comprehensive strategy aimed at safeguarding civil aviation, and passengers against cyber-attacks.
Do national cybersecurity laws take precedence over ICAO regulations?	In Singapore, the Cybersecurity Act holds precedes ICAO regulations for national cybersecurity matters, including those affecting the aviation sector. While ICAO provides international standards and guidelines for aviation cybersecurity, the Cybersecurity Act establishes specific legal requirements tailored to Singapore's needs. This Act mandates stringent measures for protecting critical information infrastructure, including those in aviation, such as incident reporting and cybersecurity defences. Despite the Cybersecurity Act's precedence, Singapore ensures its national regulations align with ICAO's global standards. This alignment allows Singapore to enforce detailed local requirements while maintaining compatibility with international aviation practices. Thus, Singapore's approach ensures robust national cybersecurity while adhering to the broader international frameworks of ICAO.
Cybersecurity sometimes falls into an organisation's IT department instead of the security team, which is usually the physical security SME instead of cybersecurity. Do you have any suggestions to bridge the gap and improve the effectiveness of the management system?	To bridge this gap and enhance the management system's effectiveness, organisations should consider integrating cybersecurity more closely with the Security team. This could involve cross-training IT and Security personnel to foster a better understanding of both physical and cybersecurity concerns. Establishing a unified cybersecurity strategy incorporating input from both departments can help align efforts and ensure comprehensive protection. Additionally, creating a dedicated role or team focused on cybersecurity within the Security department could improve oversight and coordination, ensuring that physical and digital security measures are effectively managed and integrated.
What are cyber threats?	Cyber threats are potential dangers or malicious activities targeting computer systems, networks, or digital information with the intent to cause harm. Key types of cyber threats include malware, denial-of-service DoS attacks, Insider Threats, Phishing, and Ransomware. These threats can have significant impacts, including data breaches, operational disruptions, and financial losses, driven by motives such as financial gain, espionage, disruption, or political activism. Understanding and addressing these threats is crucial for protecting digital assets and ensuring system security.

It would be good to understand what criteria/regulations each person or organisation used to assess themselves against in the survey. Different organisations from different areas of the world would likely have used different criteria.	The question is understood to question survey respondents on the relevant regulations that would apply. In the UK, specific cyber regulations are detailed on the CAA's Cybersecurity Regulation page. Different regions and sectors have unique regulatory requirements and best practices, leading to varied criteria for evaluating their cybersecurity posture or compliance. However, despite these variations, the survey results can still serve as a collective gauge of overall cybersecurity posture and compliance across diverse organisations and regions. The aggregated results provide a broader perspective on common practices, regulatory adherence, and areas needing improvement and offer a useful benchmark for understanding general trends.
How does Aviation Cybersecurity risk assessment differ from general/horizontal cybersecurity risk assessment?	In the UK, we work within the CAA's established Safety Risk Committee to understand the cybersecurity risks to aviation, ensuring the relevant subject matter experts can contribute to conversations pertaining to specific risks. This forms part of the UK CAA's Performance Based Oversight process.
How can the international community ensure that cybersecurity professionals vetted in one country/region are recognized in other countries/regions?	Aviation cybersecurity risk assessments are uniquely tailored in the context of aviation and must adhere to stringent regulations and international standards set by bodies like ICAO and National Aviation Authorities. These regulations often include specific protocols and compliance measures tailored to aviation's safety-critical environment, differentiating them from the more general cybersecurity frameworks applied across other industries.
Do you envisage a new nominated postholder, or will existing Security Managers be acceptable with support?	In the UK, each entity should nominate a Cyber Security Responsible Manager (CSRM), a person to whom responsibility has been delegated within their organisation to ensure compliance with cybersecurity regulations and to manage their organisation's cybersecurity risk exposure. Cyber Security Responsible Managers must complete the required training, complete a background check, and hold the relevant clearance. This person may hold other roles within their organisation; please contact your assigned Oversight specialist if support is required.

How is the Aviation sector ensuring there is no overlap with other sectors, such as other transport sectors or horizontal regulations like NIS2?	The UK CAA considers all applicable cyber regulations during the development/maintenance of aviation cyber-specific regulations. It works directly with the applicable government departments and sector regulators and, where possible, acknowledges equivalence with its oversight regime. Aviation adheres to specific standards set by the International Civil Aviation Organisation (ICAO) and national regulations tailored to the sector's unique needs and operational requirements. These guidelines focus on aviation security and safety, reducing the risk of conflicting with broader regulations. Within the aviation sector, defined governance structures and dedicated regulatory bodies further clarify roles and responsibilities, minimising the risk of overlapping duties. Moreover, the aviation sector also works closely with national cybersecurity authorities and the transport ministry, which aligns threat information exchanges, etc., to address potential overlaps and ensure that efforts are complementary.
Do you have any links to review what we were learning today and do further studies on your own?	Here are some useful links: • ICAO Cybersecurity - https://www.icao.int/aviationcybersecurity/Pages/Aviation-Cybersecurity-Strategy.aspx • European Union Aviation Safety Agency (EASA) https://www.easa.europa.eu/en/domains/cyber-security/regulations#basic-regulation • Federal Aviation Administration (FAA) - https://www.faa.gov/about/plansreports/faa-cybersecurity-strategy • Singapore CSA Cybersecurity Act - https://www.csa.gov.sg/legislation/cybersecurity-act
A vast amount of essential key worker information is exchanged between the Authorities and Authorised Medical Examiners (AMEs). Should Medical Record systems that are currently not fit for purpose be properly funded and developed to counter frequent failures and develop cyber resilience?	Upgrading and investing in reliable Medical Record systems will improve reliability and prevent future disruptions in the exchange of information between Authorities and Authorised Medical Examiners (AMEs).

How do you access safe current updates on new cyber scams?	To stay updated on new cyber scams safely, rely on information from trusted cybersecurity organisations such as the Cybersecurity & Infrastructure Security Agency (CISA) and national cybersecurity centres e.g. Cybersecurity Agency of Singapore (CSA), National Cyber Security Centre (NCSC) etc, which regularly provide updates on emerging threats. Reputable cybersecurity blogs and websites like Krebs on Security and The Hacker News are also valuable for current information on scams. Additionally, subscribing to newsletters and alerts from cybersecurity organisations and threat intelligence platforms offers real-time updates and comprehensive data on new cyber threats and vulnerabilities. Engaging with professional cybersecurity networks and forums can provide firsthand insights and experiences related to recent scams.
What evidence can be collected from the industry to confirm security measures are in place (instead of just ticking a checklist confirming compliance)?	To confirm that security measures are genuinely in place, rather than just a compliance formality, several types of evidence can be collected: • Independent third-party audit reports objectively assess whether security practices are effectively implemented and functioning as intended. • Documentation of past security incidents, including how they were resolved, shows the real-world effectiveness of incident response and corrective actions. • Ongoing monitoring of data from security systems, such as intrusion detection and firewall logs, demonstrates active management of security threats. • Results from regular penetration testing reveal vulnerabilities and assess the resilience of security measures. • Valid compliance certifications from recognised standards, such as ISO/IEC 27001, indicate adherence to established security criteria and regular reviews. Employee training records also offer evidence of an organisation’s commitment to maintaining security practices through continuous education.