Aviation Cyber Security Roundtable

April 11-12, 2019
Singapore, IATA Regional Office, Asia Pacific

Read Out

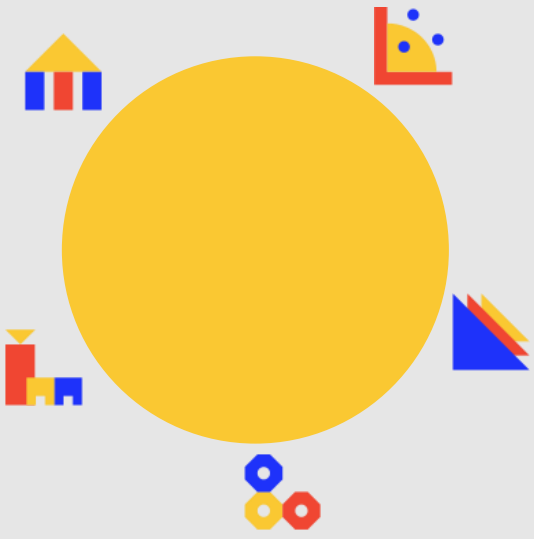

Table of Contents

Executive Summary

Background

On April 11th-12th, 2019 IATA held for the first time, at its Regional Office in Singapore, an **Aviation Cyber Security Roundtable (ACSR)** as part of its wider initiative in Aviation Cyber Security.

The Roundtable was attended by global expertise, relevant to the cyber security challenge facing the aviation sector. The participants were drawn from airports, aircraft operators, Air Traffic Management (ATM), regulators, Original Equipment Manufacturers (OEMs), cyber security service providers and more.

From the geographical point of view, colleagues from North America, Europe, the Middle East, and the Far East, including Bhutan, were represented.

Objective

The objective was to better understand and manage cyber security risk to civil aviation by collaborating across disciplines, share experience and knowledge, as well as, develop tangible actions that can help the aviation sector. IATA held five breakout groups focused on Airports, Aircraft Operators, Air Traffic Management, Regulations and Standards, and Vulnerability Management.

Over two days, the participants did not just discuss the challenges, but also looked to the future and how civil aviation could get there.

On day one, the Roundtable first shared perspectives on the current cyber security challenges facing the aviation sector, then against a 2030 timescale, what a 'good' aviation cyber security would look like was explored.

On day two, it was explored what would have to happen in order to transform the aviation sector from the 'now' to the future 2030 'vision' that was developed the previous day. Finally, the ACSR participants explored the cross-cutting issues, such as cyber security perspectives of incident and accident investigations, and collaboration with the research community.

Overall, the Roundtable found that, when it came to cyber security, the ability of the civil aviation sector was slow, even though the ability to innovate technologically was a little bit faster. This was highlighted by participants discussing the complexity of the challenges, faced by the industry, in understanding and managing a cyber security risk against a backdrop of increasing digitization and connectivity.

A quick readout of similar themes that emerged across all the focus area.

Current Perspectives

- **Scale and Complexity:** Due to the scale and complexity of cyber security risk, it is proved to be challenging to understand, prioritize and action at multiple levels.
- **We Stand or Fall Together**: Due to the interdependent and global nature of the aviation sector, cyber security incidents could rapidly scale and cause impacts internationally.
- **The Nature of Cyber Security Challenge in the Aviation Sector:** Due to the nature of the aviation sector, any cyber security incident will likely impact its reputation as much as the technology. Moreover, there is currently little public dialogue on the topic.
- **Vulnerability Management**: The inconsistencies and insufficiencies remain across the aviation sector in finding, managing and communicating about cyber security vulnerabilities, potentially leading to poor visibility of actual cyber security risk.

Future Vision – 2030

- **Cyber Security Culture:** Much like a safety culture and a physical security culture, the aviation sector has a cyber security culture that encompasses all elements of the sector, reaching from operations into the supply chain, and from the most senior levels down to the most junior.
- **Transparency and Trust:** Between all aviation sector stakeholders, there is increased transparency on cyber security issues, ranging from access to relevant data in order to secure development practices and vulnerability management. This brings a more robust level of trust between all stakeholder groups, including regulators, industry and the public.
- **Communication and Collaboration:** All aviation sector stakeholders, irrespective of geographical location, specialism or affiliation have well established lines of communication to collaborate and share cyber security relevant information.
- **Workforce:** Across the aviation sector, from its leadership to its operations and supply chain, there is dedicated enough cyber security personnel as well as sufficient cyber security knowledge instilled in aviation sector workforce.

Moving to that Vision

- **Building Consensus and Consistency:** Across the aviation sector, there is a need to build further cyber security consistency, standards, and governance. This will take organizational and individual leadership as well as a willingness for open dialogue across all stakeholders.
- **Transparency and Trust:** To build transparency and trust in cyber security, the aviation sector can apply similar approaches to what it already does across safety and security. This will bring a commonality of approach and mindset in a way that is understood by all.
- **Communications and Collaboration:** To better manage aviation cyber security risk globally, stronger relationships must be established across the aviation sector, assisted by the entities outside the aviation sector. This will then foster closer collaboration on everything, from developing best practices to managing potential vulnerabilities.
- **Workforce:** Through a dialogue of the cyber security challenges and opportunities facing the aviation sector, we can inspire a new generation of individuals and organizations that are able to support in answering the aviation cyber security challenge. Additionally, aviation personnel must be trained on how to recognize and manage cyber security risks, leading to increased vigilance and resilience.

Breakout Groups Discussion
Detailed Read Out

Airports

Current Situation

There is already a multitude of systems and stakeholders, all interdependent and interconnected, with increasing data flows across all of them. Baselining, what cyber security regulations and certifications are applicable can be challenging, especially across international boundaries, risking unequal management of cyber security risk.

A challenging discussion remains there, about how the cyber security is viewed and managed across the airports. Therefore, a concern was raised that, potentially, encompassing safety, IT, operations, and physical security, can be challenging in order to gain a full visibility of cyber security risk, especially, against the threats of cyber or physical attack.

Future Vision – 2030

The key assumptions were made, considering what the future of airport cyber security would look like, emphasizing that more connected devices, mobile or Internet of Things (IoT), and increased use of cloud computing would be present.

At the business level, there would be a collaborative 'trust' framework across airports, facilitating information sharing, and the supply chain support, both, technical and operational, with an objective of increasing the visibility and understating of risk across all stakeholders. All the airport systems would be manufactured as 'secure by design', where cyber security has been built into systems from their inception.

Further, a cyber security culture would be well established across all stakeholder, seen as a crucial element of the aviation industry. Notably, the cyber security culture would be included within innovation, procurement, recruitment, operations and all other airport areas.

What is more, access control measures across the airports would encompass innovative technology, such as biometrics, permit greater visibility and management of cyber security risk, limiting the potential for circumvention.

An information sharing on all cyber security matters, such as threats, risks, and vulnerabilities, irrespective of stakeholders, is well established, mainly, through such forums as the Aviation – Information Sharing Advisory Centre (A-ISAC).

Another key thing is an improved cyber security regulation, delivered by the leading industry organizations, namely ICAO, IATA, and ACI, providing guidance and common standards that could be followed by all stakeholders. This is not necessarily focused on details across multiple standards, but on the key elements that would have a wide applicability and commonality.

Even with the proliferation of data, where possible, the superfluous data has been minimized, which reduces the attack surface and compliance challenges.

The Roadmap to 2030

- **Airport Cyber Security Certification Program**: By 2030 an Airport Cyber Security Program should be created, which could include aspects of ISO 27002 and, developed on it, useful ACI cyber security benchmarking program. This should be scalable and applicable, irrespective of the resources or situation of each airport, with a risk assessment and mitigation as a key element of this program.
- **Developing a Positive Cyber Security Culture**: A promotion of a positive cyber security culture should be placed it the agenda of high level, impactful and relevant meetings, such as the annual ICAO regional DGCA conferences. Therefore, by 2025 cyber security is seen as a significant issue for the entire industry and stakeholders. Additionally, in the short-

term timeline, the industry should continue to promote forums and seminars that raise awareness of cyber security culture and cyber security itself.

- **Understanding and Managing Cyber Security:** By 2025 the industry should develop a methodology that permits cost and benefits analysis of cyber security, incorporating, in particular, a method to quantify the benefits of cyber security. Furthermore, this could then underpin a methodology for integrated aviation cyber security management, in conjunction with both, safety and security, management systems.

Source: IATA

- **Promotion of International Cooperation and Information Sharing:** The industry bodies should take a leadership role in encouraging and facilitating international information sharing between law enforcement agencies and stakeholders. What is more, a membership of the organizations such as ISACs should also be encouraged.
- **Improve Resilience and Availability of Airport IT Systems:** Best practice guidance, e.g. in the form of handbooks, and training programs should be developed to help airport operators improve the resilience of airport IT systems to cyber-attacks, in order to ensure better service availability and continuity.
- **Enactment of Appropriate Legislation and Regulations:** ICAO guidance on cybersecurity for airports, along the lines of the existing Chapter 18 of the ICAO Doc 8973 *Aviation Security Manual* would be highly beneficial to both, regulators and airports, greatly accelerating the progress.

Aircraft Operators

Current Situation

All aspects of aircraft operations are now connected and digitized whether an aircraft is airborne, operating at an airport or in maintenance. Additionally, the passenger journey is also increasingly digitized not only on the ground but also in the air. From a cyber security perspective, this creates a complex defensive landscape that has to deal with everything, from an insider threat to attacks against space-based assets, such as Global Navigation Satellite System (GNSS).

Overlaid on this defensive complexity is a perception that cyber security issues remained potentially siloed across regulators and authorities, making oversight and accountability, challenging. Allied to this, an emerging technology continues to shape the landscape of both, adversary and defender, as well as data integrity attacks, such as spoofing, may become more commonplace.

Future Vision – 2030

Cyber security expertise is incorporated into aviation standards bodies to ensure strong cross-collaboration and development of best practices and has also created a cadre of personnel that is able to bridge the divide.

Globally integrated regulations and standards are able to 'act faster' in response to evolving technology, even at an international level. Aligned with this, there is robust cyber security guidance for the aviation sector that is applicable at all levels, along with minimum standards, that strikes the right balance of being effective without being overly prescriptive. Additionally, there is a cyber security-aware aircraft certification process that better facilitates patching and remediation.

The critical aircraft communications are encrypted and authenticated alongside the deployment of modernized protocols. Additionally, the ability to secure and analyze aircraft, and aircraft operations, generated cyber security relevant data is low friction and standardized, facilitating a quicker insight to cyber security risk.

Cyber security principles are embedded within a safety culture, therefore an increased understanding across both disciplines is present. This cross-functional structure and information sharing also extend out to the security team, bringing a holistic view of aircraft risk.

What is more, cyber incident detection and response are designed and exercised as an integrated event between cross-functional teams and all areas of the business such as the maintenance operation center. Layering in real-time log analysis and Operational Technology (OT) monitoring allows rapid and accurate communication channels during incidents.

Taking into consideration a pilot and crew training, it incorporates cyber security perspective into operations. This is done in conjunction with a documentation (i.e., handbooks, manuals, etc.) and simulator exercises.

'Secure by design' is further matured across both, OEMs and component manufacturers, as well as there is increased transparency about cyber security measures and practices with aircraft operators. Moreover, intrusion detection systems are also deployed onboard an aircraft, able to be monitored remotely. In order to reduce the risk and likelihood of unauthorized physical access, tamper proof/tamper evident markings are in place for all critical aircraft systems.

The Roadmap to 2030

- **ICAO** must continue to coordinate global risk-based regulation on aviation cyber security whilst being informed by industry organizations, such as IATA. A gap analysis of existing industry standards, perhaps indirect to civil aviation, should also be conducted, and then, the insights should be implemented into the current isolated standards programs used by airlines. Additionally, any aviation cyber security framework that is developed, where possible, should be based on the existing frameworks, and be adjusted then to the aviation challenges.
- **IATA IOSA** – a review of possible aviation cyber security relevant standards and recommended practices via the IOSA Standards Manual (ISM) should be considered in view of the IATA Operational Safety Audit (IOSA), to enable greater insight and guidance for potential improvements to systems.

Source: IATA

- **Build a capacity** for airlines to enable, even small aircraft operators, to acknowledge how to improve and standardize their approach to cyber security. This can be facilitated by leading organizations in the aviation sector, providing guidance and templates that can be used at multiple scales or maturity levels. As part of this, a safe and collaborative discussion area for airlines, to address cyber security matters, will greatly increase the speed and depth of collaboration.

- **Vulnerability Disclosure Programs** – all aviation organizations are encouraged to put in place a coordinated vulnerability disclosure program, that creates clear pathways between themselves and any other entities that may wish to discuss a potential vulnerability (i.e. entities from within the industry or externally, for example from the research community).
- **'Secure by Design'** – standards and guidelines must be developed for all manufacturers (i.e., OEM, component or supply chain) to increase visibility and standardization. This should also incorporate the ability for frequent and agile security patching, with no impact to safety and minimal friction to deployment.

Air Traffic Management

Current Situation

Against the background of increasing data density, this was viewed from the perspective that the key activity, ensuring the data flow coming into controllers, that are processed and disseminated, is the heart of Air Traffic Management (ATM). With the amount of data and varied feeds coming into controllers, there is an increasing use of digitized decision support tools as well as increased means for greater dissemination of data and voice.

This brings an increasingly dense complexity to the role of controller against a background, where the key risk is one of adversaries disrupting access to data or its integrity. This will likely bring challenges, not just in understanding that an attack is going on, but also adequately managing both, pilot and controller, workloads during and recovering from the attacks, especially those that impact multiple systems simultaneously.

All of this was characterized through the lens of needing to maintain high quality, trusted data flows and relationships between all ATM stakeholders. In a globally interconnected industry, it was concluded that the regional inconsistencies in the approaches to maintain trust (i.e., regulations, etc.), increase friction and likely costs. Further, it was characterized that, although there are well-established processes to hand aircraft off between the ATM providers, there is no the same level of cyber security interoperation – a 'trust network'. Additionally, the difficulty of managing operational risk, whilst maintaining absolute compliance, was seen as challenging due to different objectives and processes.

Future Vision – 2030

Cyber security and resilience have been designed to ensure that a seamless passenger journey remains at the heart of that objective, bringing in such aspects like a trust, ethics, and privacy as much as security and resilience.

ATM data is pooled centrally from multiple sources into a shared repository by considerably more entities that can both create and consume ATM-related data. Feeds into this repository (i.e., data, GNSS, etc.) are varied in the levels of trust assigned to them, but the levels of trust are understood and actioned accordingly. This allows for a degree of cross-checking across all data sources, highlighting discrepancies and increasing overall situational awareness.

ATM services and its interdependencies remain resilient across the whole of the passenger journey, with robust shared visibility of cyber risk and incident management. With this in place, irrespective of any cyber disruption, the passenger journey is not adversely affected.

Where there has been increased centralization of ATM services, through such things as Remote Tower Services (RTS), this has been done with robust and well communicated cyber security measures in place. Furthermore, decision support via technology, such as Artificial Intelligence (AI), is done with transparency and the ability to prove the veracity of decisions made during both, normal and adverse, conditions.

Innovation is still strongly promoted and encouraged but cyber security, through such elements as 'secure by design', is embedded within all innovation and new products.

The Roadmap to 2030

- **Data Security Model** – it is essential to design an industry-wide Data Security Model, encompassing the criticality of data as well as where it is coming from, how it is authenticated, etc. Initially, this could be achieved by reviewing the current System Wide Information Management (SWIM) initiative, and ensuring that all cyber security measures have been

appropriately covered. In a longer timescale, ICAO should enforce a Data Security Model in order to bring global consistency.

- **'Secure by Design' Best Practices** – ICAO should ensure and coordinate that the best practices of 'secure by design' within the aviation sector are captured, regulated and disseminated in a manner that all systems can operate and scale securely.
- **Research and Development** – some key areas of research and development must be accelerated. Although a need for a high integrity location data is well understood, the proliferation of jamming and spoofing capabilities means, that further work must be addressed to ensure such activity does not impact ATM operations. The increased use of AI could have multiple benefits, this should be balanced and enable ensuing its functions, especially in safety-critical environments. Finally, finding how to embed cyber assurance into innovation is critical, if the industry is to get ahead of the cyber security challenge. This concept needs to stretch into the supply chain and be proactively collaborated on by all stakeholders, ideally to the extent that cyber security is a level playing field, not a competitive advantage. This would bring increased transparency and trust, as well as, quicker development and dissemination of best practices.

Source: IATA

- **Cyber Security Research Community Engagement** benefits need to be promoted and embedded across the aviation industry. This will lead to increased visibility of risk and vulnerabilities, as well as, likely improve processes and practices.
- **Cyber Security Competency Model** is desired across the aviation sector to help the industry better understand what cyber security knowledge the aviation operators (i.e., pilots, ATM controllers, etc.) must possess. This will facilitate better risk management and process on how to deal with cyber incidents. Aligned with this, more work needs to be addressed on developing cyber security performance measures, so that better insight incentivizes better behaviors.

Regulations and Standards

Current Situation

Considering the intensified progress and development within the aviation sector, technology, communications, and threats, it was emphasized that the regulations and standards, especially at the international level, are potentially lagging behind the reality faced by the industry. This was highlighted in, that since ICAO Resolution A39 was adopted, amongst 12,000 Standards and Recommended Practices (SARPs) across the 19 Annexes to the Chicago Convention, there remains only one standard and one recommendation relevant to cyber security incorporated in Annex 17. This poses a risk, with 193 ICAO Member States, in regionalization of standards and reducing the global interoperability that stood the aviation industry in such good stead. Allied to this, is a perspective that the nature and criticality of the cyber security risk facing the industry are currently very low, which is at odds to the perspectives of aviation cyber security experts.

Additionally, although there is a multitude of regulations that apply to cyber security in the aviation sector, there is a desire for a better understanding on the quality of these regulations, especially in the light of the challenges faced by the industry, as well as,

clarity on the best way to apply them. The highlight was also put on the need to balance between risk-based approaches and prescriptive approaches, however, with such diversity and regionality across the industry, prescriptive approaches may be challenging to enforce.

Future Vision – 2030

Regulations and standards incorporate considerations of how to motivate and incentivize the industry to improve cyber security. This avoids the risk of generating a 'compliance culture' that goes against the pro-active risk ethos of the industry.

There is a balance between prescriptive norms, minimum standards alongside principles that allow industry the flexibility to continue to innovate. Embedded within all of these are the principles that promote rapid detect and respond capabilities alongside a cyber security culture of knowledge sharing and continual cyber risk assessment. Furthermore, in the event of a cyber security incident, there is an objective root cause analysis that then enables rapid improvement of regulations, standards, and principles.

Alongside regulations and standards, there is a comprehensive oversight model that also ties in the ability to enforce improvements if required. This model is fully integrated with safety and physical security, in a way that there are no gaps of oversight and governance in risk, irrespective of the threat vector.

Although ICAO remains the overarching, global body for civil aviation, regional variations and leadership on aviation cyber security regulations and standards are in broad alignment. This is not seen as an increasing complexity but permitting the evolution of best practices that can be further applied elsewhere.

Regulations and standards have increased transparency across all aviation-related systems and data, from operations into the supply chain. This also incorporates the full lifecycle of systems, aircraft, etc., so that informed and risk-based decisions can be made throughout the entire operational life.

The Roadmap to 2030

- **Regulatory Balance**, between setting regulations first, and allowing the industry to lead and develop standards, is followed. There is a multitude of benefits in collaboratively setting regulations, however, it will take pro-active efforts between industry stakeholders and regulators, ensuring that this is both, balanced and prompt process. Working in such a manner will hopefully reduce the risk of regulations and standards being generated that are not reflective of the challenge, or where the desired levels of oversight do not match the reality.
- **Regulatory Benefits** of well-considered and drafted regulations, as well as standards, must also be clearly articulated. This will not only help on better reducing and managing cyber risk, through setting standards at the foundational level of systems and components, but it will also help in driving global and regional efficiencies, reducing the cost and friction of doing business.
- **Common Set of Cyber Security Terms** – to enable better communication on aviation cyber security globally, alongside clarity on regulations and standards, a common set of terms must be developed and agreed. This will promote the quick development of shared perspectives on cyber security issues, which will be essential in the event of a cyber security incident stretching across borders.

Source: IATA

Vulnerability Management

Current Situation

Across the aviation sector, it is challenging to know all of the cyber vulnerabilities that the industry has to manage with, therefore making it difficult to understand and mitigate the risks. Against this backdrop, there is a large number of threat actors that continually evolve attack techniques.

In the complexity of stakeholders and technology, each stakeholder has a reasonable understanding and perspective of their cyber security risk, but these perspectives are not necessarily understood or shared across stakeholders, making it difficult to gain visibility of interdependencies.

Due to the complex operational models and supplier relationships, it can be challenging to manage who is connecting to systems and for what purpose. Layered into this is that, although the industry has cyber security processes in place, their application can be somewhat inconsistent and/or insufficient. Additionally, each stakeholder is likely to apply different thresholds to, for example, investigation and mitigation across all of their processes and assets.

Against a backdrop of rapidly evolving technology, there are areas, where industry ability to adapt and manage potential cyber security issues may be lagging behind. For example, in patching critical systems such as aircraft, it is essential to perform this in a safe, agile and responsive manner, whilst minimizing downtime and maintaining safety.

Additionally, it was acknowledged that more could be done to seek insight and knowledge from outside the aviation industry. This could be from many sources, such as the research community, intra-national bodies, governmental agencies, and other sectors.

Future Vision – 2030

The industry has not underestimated a cyber security threat, or challenge it faces, and as a result, has proactively and collaboratively made significant progress in how the industry finds, assesses and manages cyber security vulnerabilities. This effort has resulted in cyber security being embedded within safety culture, and the industry is able to communicate well across all stakeholders and at all levels, including passengers.

The ability to effectively collaborate and communicate on cyber security ranges from closed, high trust environments, to the security research community. Included in this is careful but engaged public dialogue about the nature of the cyber security challenge we face and the steps being taken to mitigate them.

There is a smart regulation in place, which ensures effective and balanced compliance, generated by a strong dialogue between industry and regulators, as well as industry bodies. This encourages standards and capabilities that bring commonality and efficiency across all stakeholders. For example, applying this to threat assessment information, means that although the data and process is very similar, stakeholders are able to draw their own conclusions about the level of threat they are facing.

Cyber security training and culture are such that all personnel understands their role and responsibilities in keeping the industry safe and secure. Furthermore, the industry has built and sourced adequate numbers of cyber security personnel that can support aviation operations.

Irrespective of whether a system is OT, IoT or IT, an industry ability to quickly discover compromise and respond is world class. Layered into this, is the ability to leverage the aviation sector enormous amounts of data and apply predictive risk analysis for greater and earlier insight into risks, as well as increased consistency. As a result, incident management across the industry is effective and collaborative, irrespective of the stakeholders involved or the nature of the challenge. This is regularly exercised, as well as, lessons are reflected and applied back into the industry.

Resilience and 'secure by design' are built into all systems, so that, even in the event of compromise and trust being lost, safe operations are able to be continued. This concept has been developed into self-healing' systems that utilize both, people and automation, maximizing the potential to deal with industry challenges at scale.

The Roadmap to 2030

- **Capabilities:** As an industry, it is necessary to build consensus and then speak with one voice on the need for consistency, standards, and governance. This would include data sensitivity to safety management because both are

closely interlinked. Finally, this would ideally be reflected in regulations so that it matches the industry needs and balances regulatory requirements.

- **Personnel:** It is crucial to understand how many gaps the industry has in cyber security roles, and where those gaps are. Then, there is a need to attract cyber security talents to the aviation sector. This can be done in a number of way, such as a 'marketing plan' to highlight cyber security careers in aviation, building partnerships with academia and nations, so that the industry draw from as wide a pool as possible. To increase the cross-discipline understanding of both, aviation and cyber security, job swapping, or temporary placements can be utilized, not only within organizations but also across airports, ATM and aircraft operators. Further building relationships with academia, aviation cyber security internships and courses will also assist in bringing in high-quality talent.
- **Reducing the Costs of Cyber Security:** The power of the industry should be leveraged to create economies of scale on cyber security to ensure that it is embedded in all of the products and systems that are being supplied. This has a number of elements, such as collectively seeking cost reductions in gaining access to logs for security purposes, securing the ability to independently test security, as well as, setting and agreeing on minimum security standards for aviation systems. Ideally, this would grow into an industry consortium across airlines, ATM providers and airports that could engage with manufacturers and OEMs on behalf of their members.

Source: IATA

- **Collaboration, Culture and Communication:** By 2021 the industry collectively needs to have agreed on a vision that all stakeholders sign up to. Then, this needs to be regularly communicated and reinforced to eventually build the trust, openness, and transparency that is needed across the industry.
- **Develop and Articulate what 'Good' Looks Like:** Airports, aircraft operators and ATM providers globally, would benefit from having a clearer vision of what 'good' looks like from their perspective of cyber security. This can be generated by industry bodies working with industry leaders in cyber security, capturing their approaches and methodologies in a way that can be clearly communicated and coached to organizations that want to improve. This model of 'good' is also able to evolve with technology and threat to ensure that it remains relevant and effective.

Cross-Cutting Issues

Cyber Incident Aspects of Aircraft Incidents and Accidents

There was a wide-ranging discussion about how cyber security needed to be part of the flight safety incident and accident management process. The challenge was seen as getting access to cyber security-relevant data in a manner that permitted as near real-time analysis as possible to gain insight into potential unlawful interference via cyber means.

Other industries are quickly learning that this is a complex issue, especially against adversaries that will take considerable effort to cover their tracks. Therefore, the aviation industry should consider researching what requirements and methods are needed

to ensure that, irrespective of the system or data (airborne or not) and even post-crash, it is possible to find adversary cyber activity.

Working with the Research Community

The aviation cyber security challenge can be characterized as a race to find, manage and mitigate cyber security vulnerabilities before they can be exploited by adversaries. Across many other sectors, industry, governments, and regulators have developed productive and collaborative relationships with the research community. This resulted in the coordinated disclosure of previously unknown vulnerabilities, improved processes around 'secure by design' and improved industry standards.

But due to the high trust nature of the aviation industry and some high-profile occurrences, where researcher engagement with the industry has been poor, there remains a tense relationship between the two groups. This is likely holding back the potential for productive collaboration.

Examples were given of aviation companies that have very productive relationships with the research community and the benefits that this had brought. Fundamentally, the effort should be taken to ascertain the best way to create positive pathways between the aviation industry and the research community. This would promote good behavior on both sides and help to educate about how best each group can work together.

Conclusion

In respect of aviation cyber security that pertains to maintaining safe, secure and resilient flight operations against digital attacks, a key priority for the industry, civil aviation faces a critical challenge that still need to be addressed. Increased level of technology and digitization brings many advantages and facilitates operations. Nonetheless, it also brings risks aligned with the challenge of finding and managing cyber vulnerabilities as well as responding to cyber-attacks across the industry, including airports, aircraft operators, Air Traffic Management (ATM), regulators, Original Equipment Manufacturers, cyber security service provides, etc.

There is already a multitude of systems and stakeholders, all interdependent and interconnected, with increasing data flows across all of them. This complexity makes the aviation sector globally interdependent and vulnerable to hidden risks and ever-increasing threats. The aviation sector is an attractive target for a large number of cyber threat actors with a multitude of motivations, ranging from stealing value in data or monetary, to causing disruptions and harm.

By the main objective, to better understand and manage cyber security risk to civil aviation in a collaborative manner, share experience and knowledge, and develop a tangible actions, the roundtable identified the current aviation cyber security perspectives. It was proved that, considering the scale and complexity of cyber risk, the challenge remains how to understand, prioritize and take actions at multiple levels, especially that the scale of cyber security incidents could rapidly increase and impacts the aviation industry internationally. Due to the intensified progress and development within the aviation sector, it was also emphasized that the industry faces a challenge of inconsistencies and insufficiencies in finding, managing and communicating about cyber security vulnerabilities.

Considering the lens of where and how the industry is developing, the picture of a future vision up to 2030, in terms of cyber security, has been analyzed. This vision sets out a cyber security culture encompassing all elements of the sector, followed by transparency and trust between the aviation stakeholders. Additionally, this vision can be only achieved by a clear communication and collaboration that facilitate to share cyber security relevant information. It is also essential, that the aviation industry is provided with dedicated enough cyber security personnel.

Facing the cyber security challenges, and moving the future vision, it is encouraged that IATA, in collaboration with the aviation industry, will coordinate the process of building consensus and consistency by its governance, advocating for cyber security standards and take a leadership in conducting an open dialogue across all stakeholders, as well as, building a transparency and trust by applying similar approaches present across safety and security. It is also recommended that, the industry needs to establish stronger and better relationships, also with non-aviation entities. Finally, the industry needs to bring new cyber experts and professionals into the aviation sector as well as train the aviation personnel on cyber security issues.