WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Shaping the Future of Cybersecurity and Digital Trust
Shaping the Future of Technology Governance: IoT, Robotics and Smart Cities

Advancing Cyber Resilience in Aviation: An Industry Analysis

In collaboration with Willis Towers Watson

January 2020

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744
Email: contact@weforum.org
www.weforum.org

Contents

Foreword

Matthew Vaughan
Director, Aviation Security
IATA
Canada

Civil aviation is an incredibly safe mode of transport. Year-on-year statistics referenced by the International Air Transport Association (IATA) Annual Safety Report demonstrate this. Considering the forecast of double-digit growth over the next 20 years and the new infrastructure needed to manage capacity and services – and as indirectly evidenced by high levels of consumer confidence documented in widely available growth analysis – continued efforts today will clearly be paramount tomorrow to maintain the safety promise.

Gains in civil aviation have largely been forged thanks to the way that industry, government and the International Civil Aviation Organization (ICAO) have collaborated on the basis of empirical data. The key objective is to maintain that elusive equilibrium between regulation and risk management, to effectively enable the social contract responsibility of government while enabling industry to innovate and manage its portion of risk. Arguably, the industry is operating faster, further, more efficiently and reliably than ever before owing to the successful balance between regulatory and risk priorities. The industry embraces a philosophy of continuous improvement and seeks to understand new ways in which to manage new forms of risk and vulnerability and perhaps none more so than cybersecurity in aviation.

Noting the merits of this white paper, significant policy, regulatory and risk-based advances have been achieved for terrestrial-based systems leveraging information technology (IT). As such, IATA's approach thus far has been to focus on the protection of Operational Technology (OT) associated with the safety of flight. We acknowledge years of successful security-by-design practices led by partner original equipment manufacturers (OEMs). Additionally, certification of the airworthiness of systems has enabled advances to date. But as technology is changing, so are the priorities of aviation stakeholders and more work is required to ensure optimal resilience.

Empirically, the industry needs to continue to evaluate current risk management frameworks used by aviation and determine how fit-for-purpose they are in terms of managing cyber risk. Moreover, existing aviation safety and security cultures should be governed by a cyber strategy that is linked to evolving technology and a set of agreed principals. The ICAO Cybersecurity Strategy for Civil Aviation is a good starting point. Of the roughly 12,000 standards and recommended practices (SARPs) contained in the Chicago Convention 1944, only two deal with cybersecurity. Managing risk through policy and regulation in aviation has long been the harbinger of government, to reduce and/or remove risk altogether.

Conventional approaches alone, led by traditional aviation stakeholders, may prove to be a systemic risk to the industry itself. If not already so. The initiative of the World Economic Forum on Building Cyber Resilience in the Aviation Sector is pivotal to ensuring a continued and diverse culture of risk management in aviation based on a posture of risk, resilience and drawing from cross-sector domains. This will allow the industry, when faced with unavailable services, disruption and economic loss, to maintain continuity of services while learning from vulnerabilities and risk and to close down repeat eventualities.

As this white paper illustrates, the digital realm is omnipresent – more guidance is therefore needed in view of its accelerating development. Collaboration is our greatest counter measure yet. Just as aviation itself is interconnected across multiple jurisdictions, so too are the challenges and opportunities associated with cybersecurity. IATA fully supports the work of the World Economic Forum in this domain and looks forward to continuing our collaboration in 2020.

Executive Summary

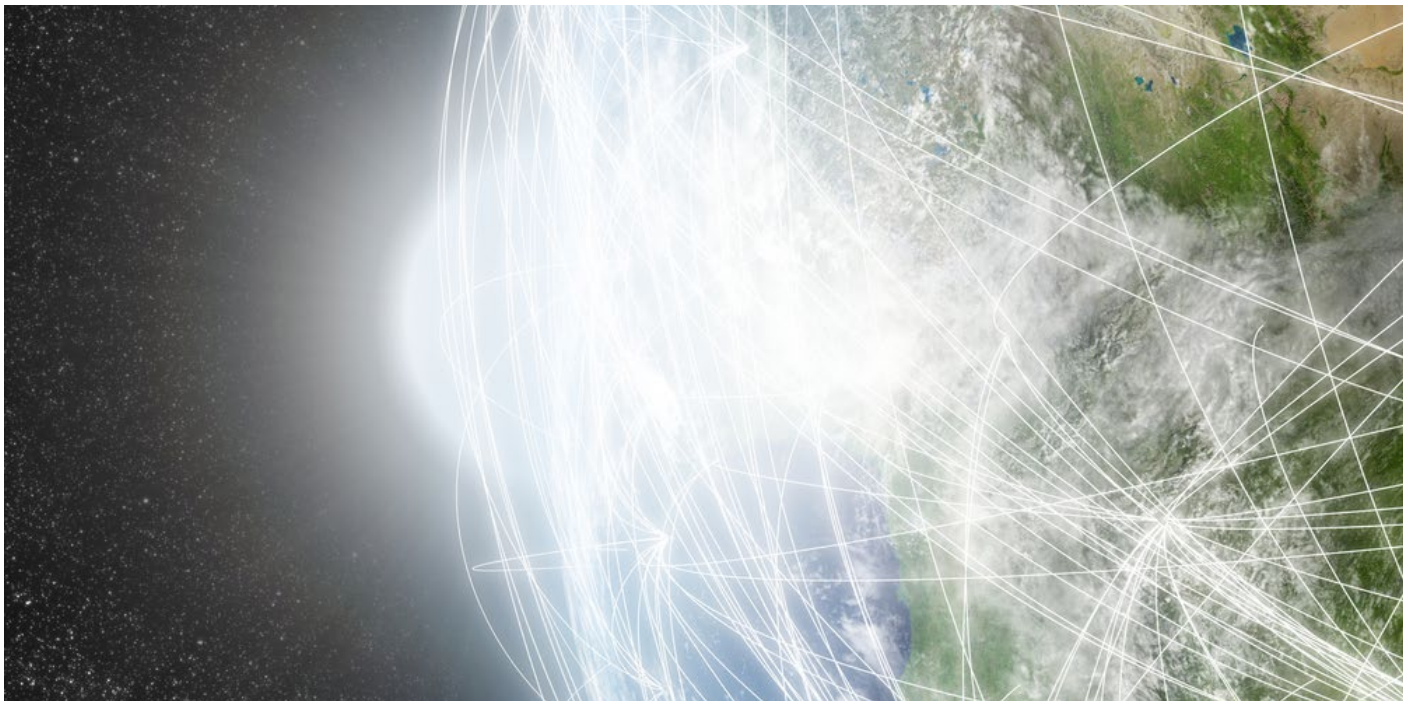
Cyberattacks are one of the top 10 global risks of highest concern for the next decade, according to the World Economic Forum *Global Risks Report 2019*, with data fraud and theft ranked fourth and cyberattacks fifth among these.

Globally, their potential cost could be up to $90 trillion in net economic impact by 2030[1] if cybersecurity efforts do not keep pace with growing interconnectedness, according to the Atlantic Council and the Zurich Insurance Group, among others. Whereas government and corporate leaders are deeply engaged in promoting effective cybersecurity strategies and global spending on security continues to accelerate, the annual number of cyberattacks globally hit an all-time high in 2018.

In January 2019, the World Economic Forum, supported by a multistakeholder community, launched an initiative to increase cyber resilience in the aviation industry. The objectives are to inform public- and private-sector leadership decisions for effective cyber risk management and to harness the benefits of the digitalization of the aviation industry. The current and future challenges to the industry are significant, and it is recognized that there are many areas where practices can be improved. Effective decision-making on risk will be critical to future success.

Cyber resilience involves more than security. It requires focus on protecting critical functions, not only assets. Cybersecurity challenges, including privacy issues, remain largely underestimated. To ensure a secure and resilient ecosystem, it is essential that public- and private-sector leaders embrace a collaborative and risk-informed approach globally, by sharing practices, insights and threat intelligence.

This white paper aims to raise awareness about the key systemic challenges to cyber resilience in the aviation industry in the context of the Fourth Industrial Revolution. Results of the study conducted in the course of 2019 in the framework of the Building Cyber Resilience in the Aviation Sector initiative (hereafter 'the initiative') indicate that the aviation industry will likely experience cyber risks similar to those of other industries grappling with new heights of digitalization and connectivity. Including multiple perspectives from public and private stakeholders, the findings presented here seek to contribute to the development of a clear and coherent vision for the aviation industry.



Based on insights from the initiative, this publication highlights the areas that warrant extra attention from public- and private-sector leaders, while recognizing the key role of the industry as well as ICAO and national authorities in bringing both leadership and vision to the challenge.

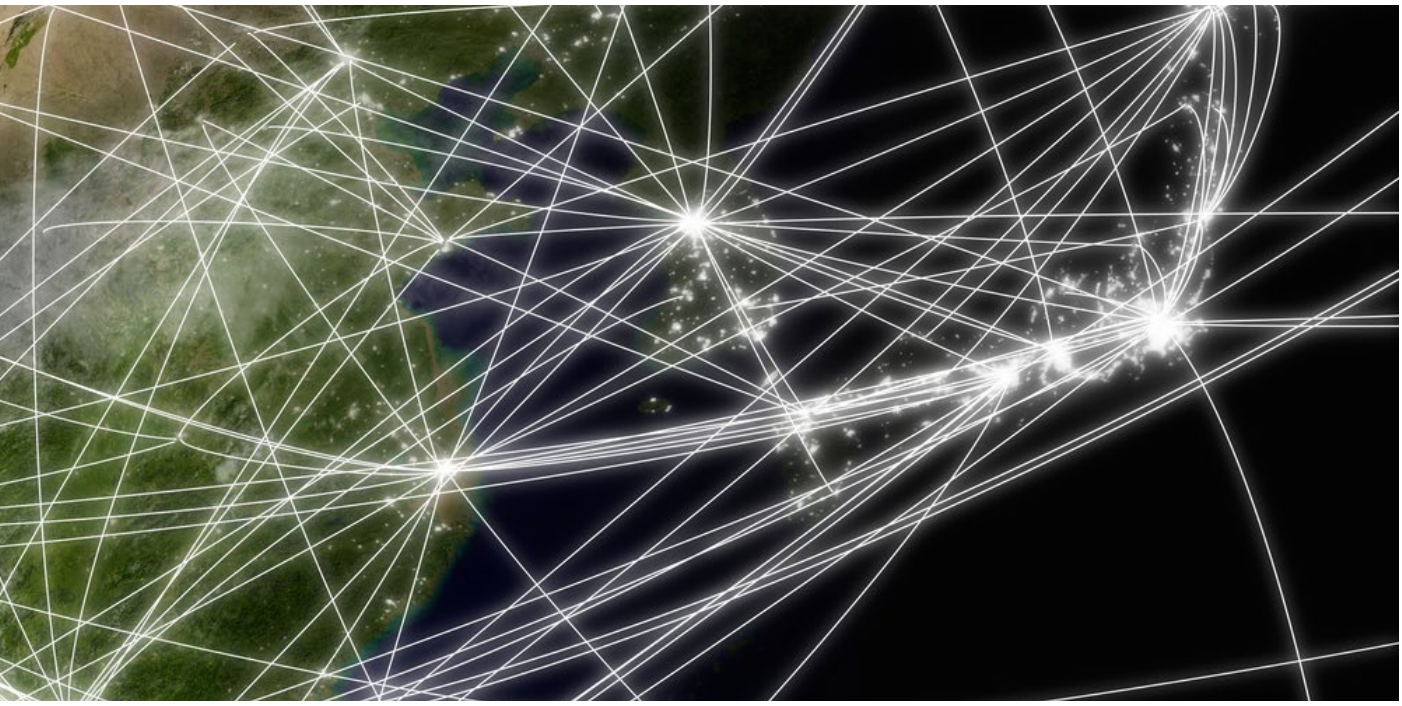
The study conducted under this initiative comprised interviews, surveys and workshops with a range of industry participants, including trade associations, regulators, air navigation service providers, airlines, airports and OEM manufacturers as well as ICT and insurance businesses working with and supporting the industry.

Gaps identified can constitute a basis for improvement and include the opportunity for collective action, the need to address people and cultural risks more effectively, the potential for improving risk decision and cyber resilience maturity, as well as the need to ensure that the multitude of best- practice frameworks and guidelines effectively address cyber risks.

Aviation industry stakeholders have multiple starting points from which to analyse where collective action is most needed to achieve cyber resilience ecosystem-wide by answering the question *When it comes to cyber resilience, what do industry stakeholders need most to address the challenges they are facing?*

Initial findings indicate the following recommended collective action:

- Building a collective approach that identifies and addresses industry challenges and gaps
- Implementing consistent and suitable methods in cyber risk management, industry-wide, to enable aviation business stakeholders in making informed decisions
- Working with the risk management, and ICT industries to develop effective incentives to encourage continuing improvement in cyber resilience
- Managing the risk associated with emerging technology effectively to increase the success of emerging technologies adoption in the aviation industry
- Foster a stronger culture of cyber resilience across the industry, including greater integration of operational and cyber skill sets within the industry



1. Aviation Industry Context in the Digital Age

1.1 Adoption of emerging technologies in the aviation industry

Today, the aviation ecosystem benefits from new levels of digitalization and connectivity. Physical things and cyber systems are becoming increasingly connected – from assets to people and data – by harnessing technologies including biometrics, artificial intelligence, machine learning, autonomous vehicles, blockchain and the industrial internet of things (IIoT).

Technological advances are creating tremendous opportunities for improved flight efficiency, customer service, security, safety operations and passenger experience – both in the air and on the ground. The opportunities that IIoT capabilities can generate for the aviation industry are unprecedented. They include operational efficiencies such as tracking and connecting airport or airline assets with maintenance and inspection functions, facility management to identify shortages or breakdowns in real time, and automation of cargo vehicles, food services, ramps and taxiways.[2]

According to the International Data Corporation, transport ranks third among the industries that will spend the most on IIoT solutions, after manufacturing and consumer.[3] Airport facility automation is expected to deliver the fastest worldwide spending growth in 2017-2022[4]. Furthermore, machine learning and artificial intelligence (AI) are becoming more sophisticated and prevalent, with growing potential to amplify existing risks or create new ones, particularly as the IIoT connects billions of devices.[5]

Yet along with the new heights of efficiency gained through increasing digitalization and connectivity come new frontiers of vulnerability. Rapid cyber capability breakthroughs also create new potential attack vectors at an equally fast pace, with researchers identifying cyber risk among the top three risks facing the transport industry globally.

The initiative to reinforce cyber resilience in the aviation sector builds on the Industrial Internet of Things Safety and Security Protocol, a co-designed framework of high-level governance principles developed by over 20 companies, governments, organizations and universities, published by the World Economic Forum in April 2018.[6]

1.2 What is at stake?

Aviation is a vital industry that contributes substantially to economic development and improved living conditions. According to the ICAO, the 4.1 billion passengers transported in 2017 are expected to grow to around 10 billion by 2040. And according to IATA, 35% of world trade by value is transported by air cargo, equivalent to $6.4 trillion of goods. The role of the aviation industry in commerce, trade and transport infrastructure makes it indispensable to the global economy.

Aviation forms part of Critical National Infrastructure (CNI) defined by the US Department of Homeland Security as "...whose assets, systems, and networks, whether physical or virtual, are considered so vital that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof"[7].

One key characteristic of CNI also apparent in the aviation industry is the high level of interdependency between the various sectors of activity (airports, air navigation services, airlines, etc.), and interconnectivity with related systems (maintenance services, network connectivity services, fuel distribution systems, etc.). One incident at any point in this value chain can have severe consequences in other areas.[8]

The probability and impact of a cyberattack on different parts of the aviation domain may vary. For instance, airports may be more vulnerable to a cyberattack than airlines, and unmanned aircraft systems (UAS) present new threats and challenges. Drones will operate differently from traditional manned aircraft and will be connected to what is called UAS Traffic Management (UTM). The drone will be connected to that platform by a form of radiofrequency spectrum and will likely operate off devices such as a pilot-in-command's cell phone. This presents many potential cybersecurity challenges, such as a drone's camera being hacked, that have yet to be addressed by the industry via a standard.

"Technology and digitization not only bring many advantages, but also risks associated with the challenge of finding and managing cyber vulnerabilities across complex, international operations from airports, aircraft operators, Air Traffic Management, and supply chain".[9] As highlighted by IATA , this complexity makes the aviation industry vulnerable to hidden cyber risks and ever-increasing threats. The airline industry is an attractive target for many cyber threat actors with diverse motives, ranging from financial gain to causing disruptions and harm, as well as unintentional motives related to human error, which are often the cause of incidents.[10]

Due to their complexity, cyberattacks on CNI may be more difficult to detect and control and may generate cascading effects resulting in economic loss, industrial disruption and, in some cases, human casualties.[11] When applied to CNI that drives economic and social progress, the impact could be severe in the absence of adequate cybersecurity and resilience measures and capabilities.

According to IATA, "the combined rapid evolution of; technology, vulnerabilities, threats and adversary motives is occurring against a background of international complexity of cybersecurity regulations, complex supply chain and insufficiently understood cyber risks across all segments of the aviation industry".[12] Moreover, cyber resilience poses a unique challenge for government regulation of businesses, as the process for certifying and enforcing good security practices can be too resource-intensive and costly for governments to address on their own.

The consequences of any major failure could carry direct public safety and national security implications and costs. Additionally, as new digital capabilities arise, balancing commercial interests with sound risk management will be even more critical to avoid significant harm to public order, confidence and trust.

Not all stakeholders are prepared for the potential risk and liability that may be brought on by new technologies. The complexity of the aviation ecosystem, with its many stakeholders, makes understanding the new nature of risk particularly challenging and highlights the strong link between digital identity management, trust and safety of operations. It also indicates the importance of identifying which aspects of the aviation ecosystem require priority attention and resources above others. The aviation industry today is realizing a future in which drones deliver packages to the doorstep and a daily commute means flying over traffic. As industry and government work together on strong policy and regulations, industry consensus standards will bring us closer to that future.

1.3 Need for global collaboration to enhance cyber resilience in aviation

The aviation industry sits within a broader geopolitical landscape that includes intergovernmental policies, security concerns, national interests, economics and society. Reaching industry alignment on meeting the challenges of new technology adoption must take these factors into account.

Without a common understanding and approach to emerging threats, industry players may struggle – and even fail – to come up with effective cyber resilience measures for the aviation industry.

To foster public-private collaboration and dialogue across the industry, the World Economic Forum has launched an initiative on Building Cyber Resilience in the Aviation Industry[13], which aims to define and address some of the salient systemic challenges confronting this industry through:

- Increasing awareness and understanding of cyber risks relative to the adoption of emerging technologies, and the impact on critical systems
- Fostering collaboration across the aviation industry to define a common understanding and approach to risk management that is holistic, risk-based and aligned across the different entities of the aviation industry ecosystem
- Helping aviation stakeholders in making informed – and more effective – decisions related to cyber risks
- Developing an industry-wide approach to cyber resilience with a multistakeholder community in alignment and collaboration with the ICAO Secretariat Study Group on Cybersecurity (SSGC), industry associations and national authorities
- Creating market incentives to prioritize capital investment for cybersecurity and resilience

To advance and help build cyber resilience in the aviation industry, the Forum has mobilized a community of experts and key stakeholders from international organizations (International Civil Aviation Organization, Organization of American States, Eurocontrol), government entities (European Aviation Safety Agency, UK Civil Aviation Authority, Israel National Cyber Directorate, UK National Cyber Security Centre), private-sector organizations (aviation, ICT and insurance sectors) and trade associations (International Air Transport Association, Airport Council International and the Industrial Internet Consortium) to identify challenges and initiatives spearheaded by various government and industry entities to enable the development of an aligned global approach.

ICAO, the industry and national authorities are currently leading many initiatives seeking to protect critical systems against cyberattacks. Likewise, there is recognition among community experts and stakeholders of:

1. The need to increase understanding and awareness of cybersecurity risks in this industry
2. The need for global synchronization of aviation cyber resilience efforts
3. The interest in gaining a common understanding, and application, of risk management practices

The goal of this community is to help promote a secure and resilient aviation ecosystem, enabling participants to transfer their industry learnings and best practices across all segments of the aviation industry that operate critical systems.

2. Aviation Industry Analysis

2.1 Global risk insights

The second most frequently cited risk in the World Economic Forum *Global Risks Report 2019*[14], was the pairing of cyberattacks with critical information infrastructure breakdown. The potential vulnerability of critical technological infrastructure has increasingly become a national security concern. The report highlighted that the disruption of operations and infrastructure resulting from cyberattacks ranked among the top five global systemic risks.

Figure 1 clearly shows the sensitivity to cyber risk among aviation industry respondents. Peers in the transportation industry prioritize "Increased security threat from cyber and data privacy breaches" higher than the aviation industry. This suggests that aviation participants find it challenging to balance cyber alongside other risks in a particularly complex operational environment as digitalization and interconnectedness become the new norm.

Figure 1 – **Transportation Risk Index**

Rank	Transportation sector	Air (All industrial capabilities providing flight above the ground, including space)	Airports
1	Increased security threat from cyber and data-privacy breaches	Failure of critical IT systems	Competition/anti-trust law scrutiny associated with M&A activity
2	Failure of critical IT systems	Competition/anti-trust law scrutiny associated with M&A activity	Change in seasonal demand, leading to shortfall or oversupply of transport (utilization/capacity) affecting prices
3	Dependence on third-party suppliers	Dependence on third-party suppliers	Failure of critical IT systems
4	Third-party security vulnerability digital supply chain resilience	Inability to keep up with pace of change and technological advancement	Extreme weather events/natural disasters, epidemics and armed conflicts
5	Competition/anti-trust law scrutiny associated with M&A activity	Over-dependence on national infrastructure	Increased security threat from cyber and data-privacy breaches

Source: Willis Towers Watson

2.2 Key insights from industry stakeholders

The impact is seen broadly across the industry, with operational disruption and legal consequences becoming more widespread, and all areas of the aviation industry experiencing losses in the last year.[15] Noting the risks that cyber threats pose for the aviation industry, including potential safety risks, industry stakeholders are developing cyber-resilience strategies to mitigate these effects and to protect critical assets and functions.

Aviation stakeholders must assess the threats against which they want to defend the industry, establish the design principles and control objectives accordingly, implement effective controls and keep them up to date. A recent survey conducted under the initiative (also referred as "the survey") examined how some members of the aviation industry view cyber risks, threats and vulnerabilities relevant to the sector. The findings shared here are representative of the surveyed community and while they have been validated by further research, they are not exhaustive. The objective of capturing and publishing these findings is to raise awareness among key aviation stakeholders as a first step to mobilizing collective action to address systemic challenges.

2.3 Threats

Cyber threats generally refer to attempts to compromise the confidentiality, integrity or availability of systems, networks or information using a data communications pathway and diverse vectors to compromise their target. This access can be directed from within an organization by trusted users, often inadvertently, or from remote locations by unknown persons using the Internet. Threats, and more importantly Advanced Persistent Threats, come from threat actors such as hostile governments, advanced cyber criminals, terrorist groups, disgruntled employees, malicious intruders, or hacktivist groups.[16] Historically, industrial control systems had a focus on availability and not confidentiality and/or integrity as those networks were typically not connected to the internet. This is changing rapidly as these systems are being connected to less secure networks and systems and could be exposed to cyberattacks targeting the weaker systems.

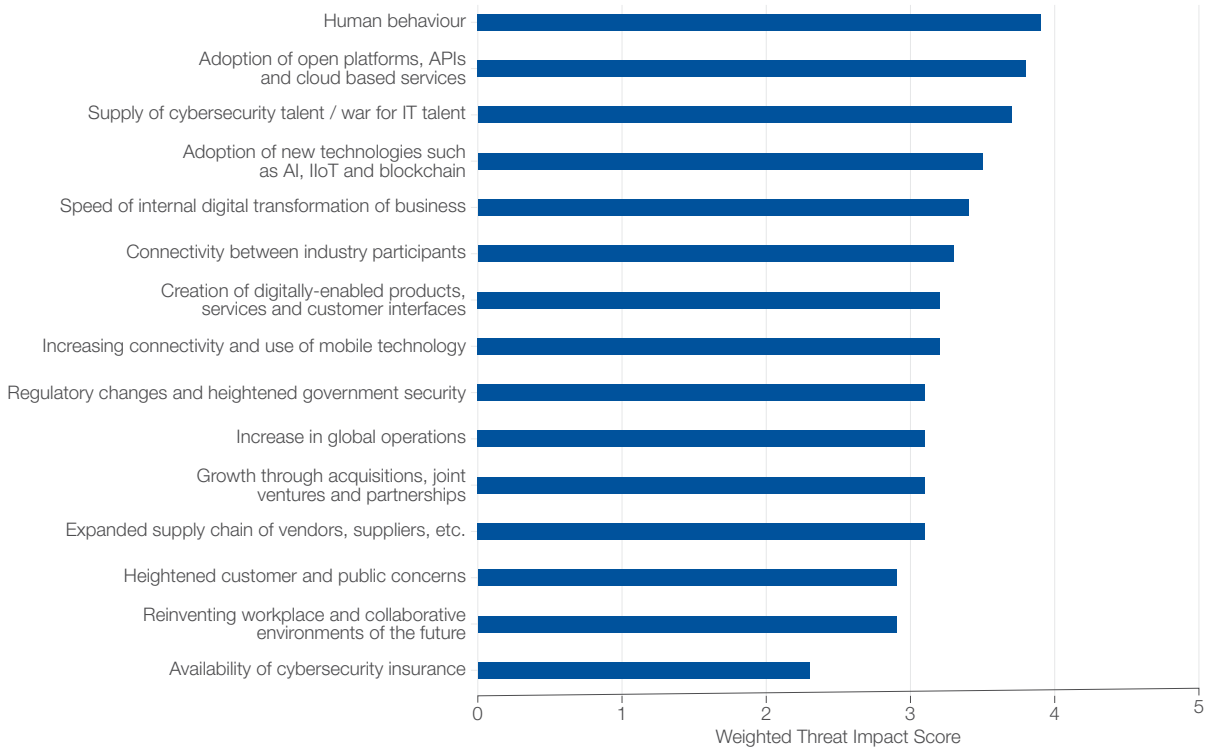
Furthermore, the threat landscape is continually changing, and new attack vectors are created at an equally fast pace. The emergence of new nation state offensive capabilities[17], able to disrupt or destroy critical national infrastructure, combined with continuing geopolitical instability and the ongoing evolution of organized crime[18] present a significant challenge for increasingly inter-connected and data-reliant industries such as aviation.

The survey analysis raises a shared concern about the ability to respond to the cyber risks.

Specifically, the role of human behaviour as a potential threat, the increasing adoption of open or shared technology platforms and the emergence of new technologies across aviation operations, combined with business transformation and talent shortages, are increasing the exposure to cyber threats (Figure 2).

Renewed concern over human behaviour as both a threat and vulnerability is apparent across multiple sectors with 87% of executives around the world citing untrained staff as the greatest cyber risk to their business.[19]

Figure 2 – **Perceived impact of emerging issues to the aviation industry**



2.4 Risks

World Economic Forum research on *Understanding Systemic Cyber Risk*[20] explained that "systemic risk is inherently different from non-systemic risk in that the consequences are more widespread – systemic risk is the risk of 'breakdowns in an entire system, as opposed to breakdowns in individual parts and components' – and more complex as multiple variables, connections, dependencies and interdependencies result in cascading, often unexpected, consequences". The industry challenges associated with systemic risk are consequently also increasingly interconnected, widespread and complex.

In addition to the risk insights disclosed by the survey, the following challenges were prioritized by initiative aviation community members meeting in November 2019:

1. Highly interconnected/interdependent supply chain
2. Global synchronization of aviation cyber resilience efforts / initiatives
3. Developing an aviation cyber resilience culture across the entire industry
4. Building coherent understanding of cybersecurity risk across safety, physical security and enterprise
5. Aviation cybersecurity workforce development
6. Increasing objectivity and transparency of aviation security risk

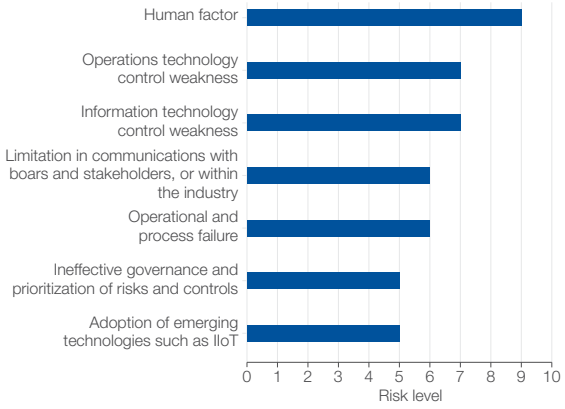
While industry-wide survey participants highlighted connectivity and technology change, individual organizations considered the human factor to be the primary risk concern for them. Awareness of this risk factor has increased, yet there still is an industry need to further develop a comprehensive cyber culture.

As Willis Towers Watson and ESI Thought Lab emphasized in 2019, "Leaders in cybersecurity are devoting significant resources towards protecting IT and risk functions within their organizations against external threats, but employee processes and training as well as corporate culture play a more integral role than many realize."[21]

Techniques used during risk assessment impact the ability to evaluate the extent of risk associated with an organization's perceived threats. When asked about the assessment techniques used, nearly 75% of survey participants reported using qualitative techniques, with the remainder using semi-quantitative techniques such as assigning financial exposure values in risk register.

As industry risk-management practices become more mature, a more quantitative approach to risk management may be introduced, to better understand the risks associated with these threats and to build a more resilient industry.

Entity level risks



Source: Initiative survey results, Willis Towers Watson

Sector level risks

Source: Initiative survey results, Willis Towers Watson

2.5 Vulnerabilities

Vulnerability can be understood as "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat actor".[22]

Most participant organizations were willing to share the type of incident(s) incurred within the previous 12 months. This knowledge and the practice of sharing breach information helps provide a basis for identifying where key vulnerabilities lie. By understanding the incidents that have occurred, the industry is able to recognize where attackers are targeting and can begin building more resilient controls.

Most interestingly, human vulnerabilities were most commonly cited, with most participants reporting incidents emerged from social engineering. Despite organizations identifying increased interconnectedness as a salient threat, the vulnerabilities associated with attacks on an organization via partners, customers, vendors and intermediaries ranked low in comparison.

Figure 3 further evidences the prominent role of employees and the human factor driving cyber incidents. Claims to insurers by breach type highlight the consistent involvement of people and cultural factors, showing an impetus for controls to be built around the human and culture elements within the ecosystem.

Frequency of cyber incident occurrences in 2019

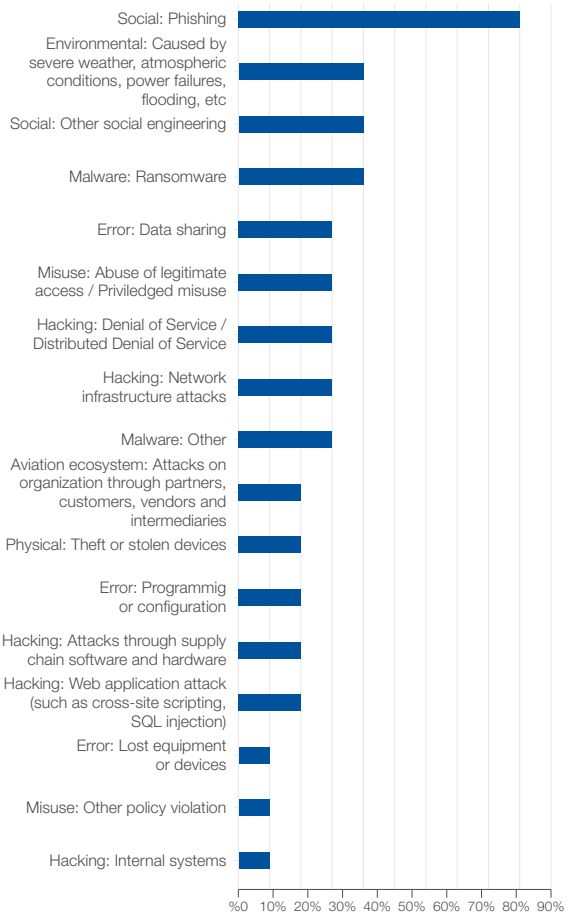
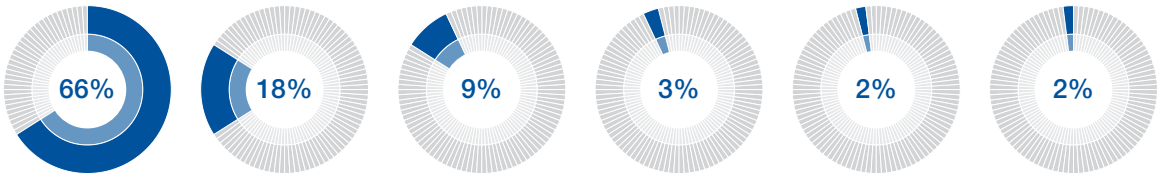


Figure 3 – **Percentages of claims by breach type**



Claims experienced by insurers
Source: Willis Towers Watson – Claims data[23]

Based on analysis of the insights obtained in this initiative from interviews, the survey and community interactions, the Forum has identified three primary domains of focus where collective action can be improved to identify and manage cyber risk: People and Culture ("People"), Capital and Risk Management ("Capital"), and Technology and Operations ("Technology"). These areas are the focus of subsequent sections of this publication.

3. Identifying and Managing Cyber Risks across People, Capital and Technology

The primary domains of focus that have been identified as a priority are presented with the salient challenges within the domain, collective action considerations to address some of these challenges and key questions that leaders and practitioners are encouraged to address collectively to arrive at a common understanding and potential actions to improve cyber resilience in the aviation sector.

3.1 Common methodologies

Cyber resilience can be enhanced by a wide range of approaches, methodologies and toolsets that can be used by organizations to assess, monitor and manage their security posture.

There is abundant guidance in the cybersecurity community from well-accepted government and industry standards for information security globally. These include NIST SP 800-30[24] and ISO/IEC 27005:2018[25], as well as controls-oriented standards such as the NIST Cyber Security Framework[26] and ISO/IEC 27001:2013[27], and assurance frameworks such as the UK NCSC's Common Assurance Framework[28]. A snapshot of the diverse applicable frameworks is shown in Figure 4.

Beyond this diverse set of tools, a variety of industry and national standards, guidance frameworks and technology-specific standards comprise a complex landscape of legislation, regulation, and guidance. Yet the application of the guidance continues to fall short of what is required to ensure effective defense against cyberattacks.

Figure 4 – **Common methodologies**

Strategic approach

Enterprise Risk Management (ERM)

International Organization for Standardization (ISO)		National Institute of Standards and Technology (NIST)	
Framework and maturity level – ISO 31000:2018 – ISO 29100:2011 (Privacy)	**Taxonomy and risk assessment** – ISO 31010:2011	**Framework and maturity level** – RMF:2019 & SP 800-37:2018 – Privacy Framework:2019	**Taxonomy and risk assessment** – SP800-30:2018

Tactical approach

Information Technology (IT)		Operation Technology (OT)		Aviation / CNI Specific
ISO	**NIST**	**ISO, IEC**	**NIST**	**NIST**
Maturity level – ISO 27001:2014 – ISO 27002:2013 – ISO 27017:2015 (Cloud) – ISO 27018:2019 (Cloud Privacy) – ISO 27031 (BIA) **Taxonomy and risk assessment** – ISO 27001:2014	**Maturity level** – CSF 1.1:2018 – SP 800-53 (Draft) **Taxonomy and risk assessment** – A Taxonomy of Operational Cyber Security Risks Version 2 (CM:2014) – FISMA, SP 800-53 & OCTAVE	**Maturity level** – IEC 62443 (1-1, 2-1, 2-2) – ISO 27019:2017 **Taxonomy and risk assessment** – IEC 62443 (3-1, 3-2, 3-3) – ISO 27019:2017	**Maturity level** – SP 800-82 Rev.2 – CSF 1.1:2018 – SP 800-34 (BIA) **Taxonomy and risk assessment** – SP 800-82 Rev.2 – SP 800-53 (Draft)	– NCSC CAF – CAP 1753

Operative approach

Information Technology (IT)				OT and Critical Infrastructure			Aviation	
– MAGERIT	– EBIOS	– SP 800-30	– RISK IT	– EPCIP	– CARVER 2	– BIRR	– NPA 2019-07	– NPA 2019-01
– CORAS	– CRAMM	– TARA	– OCTAVE Allegro				– EC 2015/1998	– EC 300/2008

Technical approach

Information Technology and Operation Technology (OT) and Critical Infrastructure

– FMEA	– FMCA	– FTA	– ETA	– DRBFM	– HAZOP	– HACCP	– SWIFT

Source: World Economic Forum and Willis Towers Watson

The World Economic Forum with its partners have worked to consider the current barriers to the adoption of these practices to provide some key essentials to organizations wishing to improve their ability to defend against attacks. In 2019, the Forum published *The Cybersecurity Guide for Leaders in Today's Digital World* for senior executives who are responsible for setting and implementing the strategy and governance of cybersecurity and resilience in their organization.[29] Cybersecurity is everyone's responsibility in an organization, not solely that of the Chief Information Security Officer (CISO). It is essential that key C-Suite executives such as Chief Information Officers, Chief Technology Officers, Chief Digital Officers, Chief Financial Officers and other company leaders understand their cybersecurity responsibilities.

Looking at the barriers to adoption of cybersecurity best practices, current approaches make it difficult to implement comprehensive best practices across the full spectrum of the digital and operating environments in organizations. Second, security tools and processes are often set up and then forgotten, consequently and quickly becoming redundant in a continuously evolving threat landscape. Systems must be updated continuously to keep pace with the flow of business activity if they are to protect effectively against newly discovered vulnerabilities. Third, although organizations have many tools in place to automate security tasks, the tools often can't be used in concert in a fully automated fashion. This results in a complex landscape of security tools, gaps and vulnerabilities and, ultimately, in the inability to deploy a holistic automated approach. A major final challenge is the sheer volume of work involved in following up on security alerts and incidents – and that cannot be automated. There is significant reliance on humans to carry out security functions, in particular to assess the more strategic implications of alerts and incidents. The shortage of cybersecurity talent, however, means this capability is often under-resourced. To offset these challenges, organizations need to consider outsourcing some of the more advanced, complex and onerous services to service providers, depending on their risk profile, to improve their coverage and service-level agreements.

The role of an organization's cyber-resilience leaders is to support the mission of their organization by ensuring that cyber risks are managed at an acceptable level, as defined by their organization. It is unrealistic for any organization to expect to achieve faultless security, or even to consider this possible. No enterprise is immune to cyber threat and organizations need to anticipate that a compromise will occur. The end goal is resilience, which we define as the ability to quickly and efficiently identify and minimize the impact of an incident so as to allow an organization to continue its mission as effectively as possible. In the digital age, organizations must continuously adapt their cybersecurity measures in proportion to the growing number and sophistication of the threats they face.

Recommendations for collective action

1. Implement consistent and suitable methods in cyber risk management, industry-wide, to enable aviation business stakeholders in making informed decisions
2. Rather than adding to the complex cyber framework landscape, stakeholders' capabilities need to be enhanced to:
   - Ensure all stakeholders can focus on what matters most, while at the same time ensuring that risk areas beyond IT are also addressed
   - Enable organizations to successfully align operational security needs and priorities with board level decision making
   - Promote a synchronized approach to cyber resilience global efforts

3.2 People and culture

Concluding from the survey insights, aviation, like many other industries, is at risk of focusing too heavily on IT systems and infrastructure, and insufficiently on the people that operate and interact with such systems.

As the aviation industry focus evolves from "cybersecurity" to "cyber resilience", people and workforce considerations are becoming particularly relevant.

As above, when asked to prioritize 14 industry challenges, community members ranked Developing an aviation cyber resilience culture across the entire industry as the third most important issue, and Aviation cybersecurity workforce development as the fifth. These issues have been recognized by the global community. ICAO's 2019 Aviation Cybersecurity Strategy recognizes and addresses this, citing capacity building and cybersecurity culture as key components of an effective cyber resilience programme. In the Strategy, ICAO states that "the civil aviation industry takes tangible steps to increase the number of personnel that are qualified and knowledgeable in both aviation and cybersecurity".[30]

This is an important step, but more must be done. The aim should be to not only attract engaging and retain qualified cybersecurity professionals, but also to build a higher degree of "cyber IQ" for all stakeholders and employees in an organization, particularly operational staff interfacing with critical systems. Companies experiencing cyber breaches lack the following aspects of employee experience, either significantly or entirely:

- Purpose tied to customer centricity – responsiveness, anticipating needs, optimizing processes
- Work marked by speed and flexibility in making decisions and managing teams
- People practices that empower staff through voice, respect and support for teamwork
- People practices that stress training and development, and align pay with performance

In view of the above, there are several key strategic challenges for the aviation industry related to human factors that should be included in industry-wide cyber-resilience initiatives.

Meeting these challenges will be a crucial industry focus in the next few years. As organizations embark on that journey it is worth noting that the industry has done an impressive job of building a safe industry. Concepts such as "just culture" within the airline sector have proven highly effective at driving better safety outcomes. The implication here is that if the aviation industry applies the same approaches to building a cyber-resilient culture as it has to a safety culture, significant advances can be expected.

Recommendation for collective action

Foster a stronger culture of cyber resilience across the industry, including greater integration of operational and cyber skill sets within the industry.

A common understanding of cyber culture within organizations and across the industry can improve stakeholders' ability to:

- Address the perception gap between employees, IT and Cybersecurity departments and the C-Suite, on who owns the issue and where accountability and responsibility lie
- Make sure individuals are equipped with the tools to manage cyber risks with the same level of confidence that they manage other risks
- Ensure emerging leading practices become part of the standard set of board competencies
- Align and embed desired behaviors into wider organization culture, rather than solely through point-in-time training that is often forgotten

Beyond the challenges to individual organizations, cyber risk is a systemic challenge and cyber resilience, a public good. Each organization acts as a steward of the information they manage on behalf of others. And every organization contributes to the resilience of not only their immediate customers, partners and suppliers, but also to the overall shared digital environment.

For these reasons, the World Economic Forum developed an important resource in 2017, *Advancing Cyber Resilience: Principles and Tools for Boards.*[31] The results of an extensive process of co-collaboration and consultation, this publication has distilled leading practice into a framework and a set of tools that boards of directors can use to integrate cyber risk and resilience into their organization.

Key questions to improve cyber resilience

1. How would your organization build industry-wide understanding of the elements beyond technology, such as human factors and organizational culture, that have the greatest impact on cyber resilience?

2. How would you extend the information-sharing culture in aviation safety to the cybersecurity domain?

3. Which consistent and clear processes does your organization need to monitor, measure and improve the cultural and people factors that impact cyber resilience?

4. How could you more closely embed HR/ Training and Development functions within core teams responsible for cyber resilience, and set guidelines for cyber relevant human factors training that work?

5. What guidelines would you have for talent management that incentivize and reward appropriate cyber behaviour for all staff, not just cyber and IT professionals?

3.3 Capital and risk management

One of the recurring themes expressed in the community during the research conducted is the challenge of aligning cybersecurity operational decision-making with board-level executive decision-making. This is corroborated by additional research: Some 96% of board members believe they should spend more on cyber than they do now[32], while security leaders are no happier: many would not expect their board to help if a significant incident occurred, with high post-incident job turnover amongst this group. Indeed, a growing minority self-medicate to handle the stress of the job.[33] Seventy-five percent of survey respondents used qualitative methods only (such as ranking risks high to low, or red to green), 25% had investigated semi-quantitative methods (such as assigning risks on simple ordinal scales from 1 to 5, or using predetermined tables as per NIST SP800-30). At the time of writing (December 2019), based on survey responses, interviews and workshop contributions, no respondents had declared adoption of quantitative methods such as OpenFAIR[34], QIRA[35], LossPIQ and CyberQuantified.[36]

Where cybersecurity leaders are using qualifiers like “high” or “low” to describe risks (or ranking them using simple ordinal numbers) this can often be misleading and subject to misinterpretation, challenging effective decision-making processes unless there is some indicative financial impact based on the levels. Simple questions such as “How much will our organization’s risk exposure improve as a result in this investment?” or “What is the optimal investment in implementing or improving security controls? ” remain hard to answer, contributing to misalignment of perspectives between security leaders and boards and possibly making investment decisions harder to justify.

As long as this communication gap exists, it is likely that the views of security leaders and boards will continue to be misaligned, and security investment will fall below (or only occasionally above) the optimal level to manage cyber risk effectively while meeting other goals of the aviation industry – such as growth, commercial viability, response to other risks such as oil price fluctuations and economic recession.

Key questions to improve cyber resilience

1. How would your organization effectively incentivize risk-based improvement in cyber-resilience practices, instead of a compliance-based approach, and develop outcomes that enable organizations to move up the "cyber-risk maturity ladder", within commercial, operational and safety constraints?

2. How does your organization measure the expected likelihood and impact of events for each critical risk scenario? Does this provide you with sufficient visibility?

3. How do you know that your organization is receiving a positive return on investment from cybersecurity expenditure, and that a better return could not be achieved with a different, improved, control strategy?

4. What robust understanding and metrics could be developed to measure and report on cyber resilience, specific to aviation, allowing for organization size, location and function?

5. How can your organization improve cybersecurity coordination across international boundaries and through the supply chain?

Collective Action Consideration

1. Manage the risk associated with emerging technology effectively to increase the success of emerging technology adoption in the aviation industry
2. Align operational security needs and priorities with board-level decision-making to accelerate risk-informed decisions. Stakeholders depend on their success in:
   - Developing a common taxonomy a and clear statement of risks between the risk management (IT and OT) and C-Suite stakeholders, ensuring and end-to-end process
   - Promoting the adoption of quantitative methods on a sector basis (often referred to as Cyber Risk Economics)
   - Establishing risk management disciplines for better alignment of risk and investment on an entity, sector and global level
   - Planning, embedding and incentivizing cyber resilience measures in capital investment cycles

3.4 Technology and operations

The Operational Technology (OT) environment can be defined as "the hardware and software dedicated to detecting or causing changes in physical processes through direct monitoring and/or control of physical devices".[37] In the aviation industry, this would include the control systems necessary for aviation operations and safety.

Differences between general information technology and operations technology systems are significant, driven by a number of factors including, but not limited to, the high capital cost of hardware and a critical need for resilience. As a result, OT solutions tend to be less frequently updated and more likely to host obsolete or unsupported software and operating systems. This poses a different set of challenges, as does the relative lack of standardization compared to IT environments. While standards are emerging that respond to the OT challenge they do not yet take into account sector-specific considerations. For example, standards may require retention of audit logs for cybersecurity purposes but may not consider logging requirements to a Flight Data Recorder ("black box"). It is likely that equipment and technology infrastructure being implemented today will continue to be in operational use many decades into the future, increasing the importance of a "security by design" approach and implementation of effective baselines and open standards.

This digital landscape in the aviation industry is made more complex by new technologies such as IIoT, AI or 5G, the vulnerabilities of which are often misunderstood, as these change not just the systems used by aviation organizations but also the interfaces across the value chain. As these systems also become critical to operational efficiency and safety in the future, the need for resilience may well exceed the requirements placed on system manufacturers today. Therefore, industry participants need to evaluate not just the controls needed today, but also those that will be required in the future.

Current approaches to enforce technology controls tend to focus primarily on two of the three pillars of cybersecurity: confidentiality (the risk that systems of information will be available to the wrong people) and to a lesser extent, availability (the risk that systems of information will not be available when needed).

While best practice framework and standards focus on all the Confidentiality, Integrity and Availability pillars, integrity related controls are more complex to enforce and manage. Attacks affecting the integrity of information poses an increasing risk to the aviation industry. Machine learning will bring new risks related to data security such as data poisoning, data manipulation, logic corruption or data injection.

Compromise of aviation systems resulting in incorrect data flowing between aircraft, aircraft maintenance organizations, airports and air navigation systems could have a critical impact. Also, it is possible to envisage scenarios where a cyberattack against the integrity of systems or information could compromise the safety of an aircraft or airspace, or underline public confidence.

Recommendations for collective action

1. Work with the risk management and ICT industries to develop effective incentives to encourage continuing improvement in cyber resilience
2. Ensure the resilience of the digital aviation landscape via stakeholder collaboration across an interconnected supply chain to:
   - Embed cybersecurity and resilience in the design of connected devices and systems
   - Take a holistic and risk-based approach to defend and respond to new cyberattacks that will increase in complexity, frequency and volume
   - Understand shared risk ("your risk is my risk") and develop market incentives to nudge industry players to improve cyber capabilities across the supply chain

Key questions to improve cyber resilience

1. Does your organization's approach to information, cyber and IT risk management take full consideration of the risks posed by emerging technologies such as IIoT?
2. Does your organization understand the impact of emerging technologies on its attack surface – both outside and within the organizational and network perimeter?
3. Does your organization's cyber resilience strategy, risk scenarios and incident planning exercises take full account of system and data integrity risks, as well as confidentiality and availability?
4. With ongoing changes in connectivity, technology and business practices how do your organization's cyber and safety risks interconnect?
5. Does your organization have a clear understanding of the risk posed by its supply chain and partners across the aviation ecosystem, including manufacturers, support partners and infrastructure operators?
6. How can your organization develop and maintain effective baselines of cyber capability?
7. How can your organization continuously monitor cyber risks?
8. How can your organization build an industry database that enables minimum standards to be set, and industry-wide leveraging of best practice?

4. From Insight to Foresight

While different requirements, standards and approaches are currently being implemented to assess, manage and mitigate cyber risk, there is still a long way to move from reflection to action. The vision of a prosperous, digitalized and resilient aviation industry can fully materialize if stakeholders can find practical solutions.

The first step is to promote and enhance common industry definitions, many of which have already been established by ICAO. Moreover, industry stakeholders must engage in a constant dialogue to share information – and ideally arrive at shared conclusions – about threats, risks, impact and best practices.

A successful cybersecurity strategy and its implementation are dependent on the culture of the organization. Cybersecurity, privacy and digital trust are all based on how well the organization manages to integrate security as an inherent part of its DNA. The importance of fostering an environment of security and risk awareness, shared ownership of cyber risk and cyber risk resilience is only going to grow. Cybersecurity leaders in the aviation industry who are able to step beyond a tactical, technical level are more likely to gain credibility and support among leaders across the organization, including the board, C-suite and business unit leaders. In the Fourth Industrial Revolution, all businesses are undergoing transformative digitalization of their industries that will give access to new markets, as well as opportunities for a better and more prosperous world. The digital transformation is powered by disruptive technological advancements such as 5G, AI, Cloud computing and the connection of the physical world to the digital through IoT technologies that will connect everything, generate petabytes of data, and increase the attack surface and number of attack vectors.

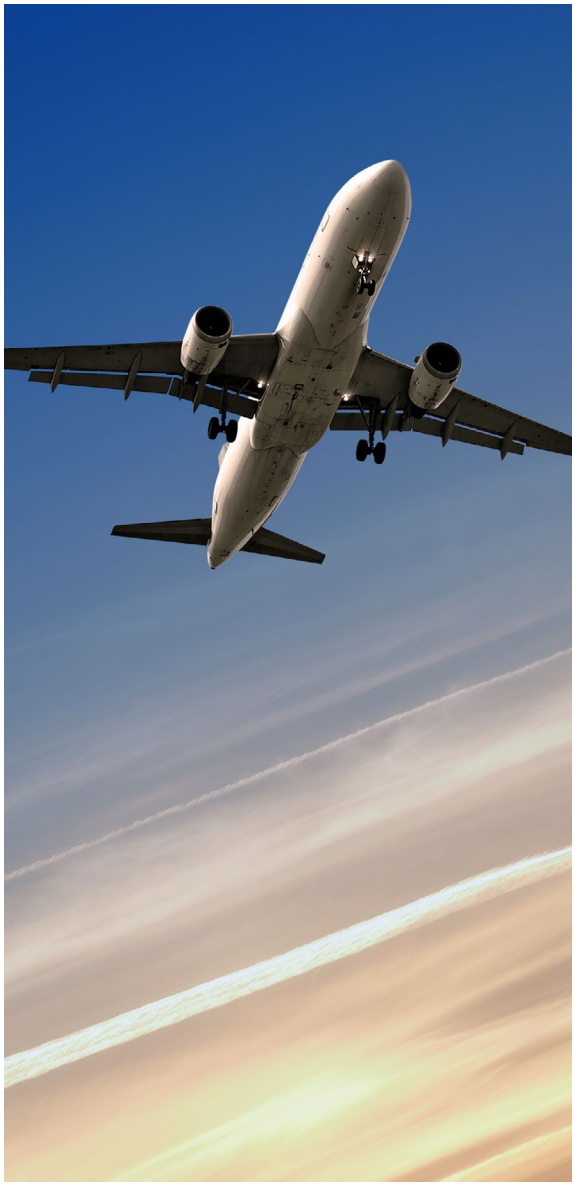
As customer data, intellectual property and brand equity evolve, they become new targets for theft, directly impacting shareholder value and business performance. In response, business leaders need cybersecurity leaders to take a stronger and more strategic leadership role. Inherent to this new operative is the imperative to move beyond the role of compliance monitors and enforcers to better integrate with the business, manage information risks more strategically and work toward a culture of shared cyber-risk ownership across the organization.

When assessing cyber risks, cybersecurity leaders are now called upon to assess their business impact and apply metrics to measure their operational, regulatory compliance and financial impact. Like in the physical world, perfect security does not exist in the digital world – trade-offs must be made. Businesses and key stakeholders need to make better

informed decisions on the risk appetite of their organization to define a good enough cybersecurity posture. This involves assessing the threat landscape, the attackers' motives and tactics as well as identifying critical digital assets, known vulnerabilities to prioritize the appropriate level of controls required with regard to people, processes and technologies. Strong cybersecurity has become fundamental to a resilient business and industry ecosystem. With effective cyber-risk management, businesses can achieve smarter, faster and more connected futures, driving business growth. As the cyber threats to business continue to evolve, public- and private-sector leaders will have to address them in the digital and physical worlds, to mitigate any potential harm to individuals and avoid the disruption of critical services.

The World Economic Forum's ambition is to continue collaborating with the key global stakeholders in aviation to develop a widely-accepted approach that can help build cyber resilience through its initiative Building Cyber Resilience in the Aviation Sector and promote further collaboration with public and private partners. This paper is the result of the initiative's first phase – research and landscape analysis – and the starting point of the second phase – developing a common approach for the aviation industry – which will take place in 2020.

The Forum will continue to support the aviation industry by engaging a multistakeholder community to co-design and pilot a common approach and methodology which will be shared with the Forum's policy community in 2020.



Contributors

Lead Authors

Andrew Hall	Global Client Relationship Director, Willis Towers Watson, UK
Jake Wingfield	Cyber Risk Associate, Willis Towers Watson, UK
Georges De Moura	Head of Industry Solutions, Platform for Shaping the Future of Cybersecurity and Digital Trust, World Economic Forum
Karime Kuri Tiscareno	Project Lead, Platform for Shaping the Future of Technology Governance: IoT, Robotics and Smart Cities, World Economic Forum

Contributors

Lucas Kelly	Chief Information Security Officer, Corporacion America Airports, Argentina
Yoshi Parlevliet	Cyber Risk Specialist, Deloitte, Belgium
Andrea Radu	Director, EMEA Cyber Strategy, Deloitte, Belgium
Chris Verdonck	Partner, Deloitte, Belgium
Thomas Heuckeroth	Chief Information Security Officer, Emirates Group, UAE
Patrick Mana	Cybersecurity Cell Manager, Eurocontrol, Brussels
David Mabry	Chief Information Security Officer, Gulfstream Aerospace Corporation, USA
Pascal Buchner	Chief Information Officer, IATA, Switzerland
Matthew Vaughan	Director Aviation Security, IATA, Canada
Claire Zaboeva	Senior Strategic Cyber Threat Analyst, X-Force IRIS, IBM Security, UK
Julian Meyrick	Managing Partner & Vice President Security Strategy Risk & Compliance, IBM Security, UK
Saulo Da Silva	Chief Global Interoperable Systems Section, Air Navigation Bureau, ICAO, Montreal
Jesus Molina	Co-Chair Security Working Group, Industrial Internet Consortium, Spain
Dadi Gertler	Technology Alliances Manager, Cyber Technology Unit, Israel National Cyber Directorate, Israel
Zenia Laxa	Cyber Security Engineer, San Francisco International Airport (SFO), USA
Ian Law	Chief Information Officer, San Francisco International Airport (SFO), USA
Christian Keller	Head of Information Security, Swiss Airlines, Switzerland
Laurent Kettela	Head of Cybersecurity & Transformation Program, Thales Group, France
Peter Drissell	Director Aviation Security, UK Civil Aviation Authority, UK
Nicky Keely	Head of Cybersecurity Oversight, UK Civil Aviation Authority, UK
Crispin Marriott	Global Client Relationship Director, Willis Towers Watson, UK
Matt Palmer	Senior Director, Cyber Risk, Willis Towers Watson, UK (2017-2019)

Glossary

IIoT: The Industrial Internet Consortium defines the industrial internet as an "internet of things, machines, computers and people, enabling intelligent industrial operations using advanced data analytics for transformational business outcomes"[38]. IIoT is broad in focus but can perhaps most easily be understood as the application of IoT technologies in an industrial or business environment, as opposed to individual consumer setting.

Threats: Cyber threats refer to attempts to compromise the confidentiality, integrity or availability of systems, networks or information using a data communications pathway. This access can be directed from within an organization by trusted users or from remote locations by unknown internet users. Threats can come from numerous sources and can include threat actors such as hostile governments, terrorist groups, disgruntled employees, and malicious intruders.[39]

Systemic Risk: "Systemic risk is inherently different from non-systemic risk in that the consequences are more widespread – systemic risk is the risk of 'breakdowns in an entire system, as opposed to breakdowns in individual parts and components' – and more complex as multiple variables, connections, dependencies and interdependencies result in cascading, often unexpected, consequences".[40]

Vulnerability: "Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source".[41]

Endnotes

1. 2015. Mitigating cyber risk could make a difference of USD 120 trillion to global economy by 2030. https://www.zurich.com/en/media/news-releases/2015/2015-0910-01 (link as of 15/01/2020)
2. 2018. Industrial Networking Enabling IIoT Communication. Industrial Internet Consortium. https://www.iiconsortium.org/pdf/Industrial_Networking_Enabling_IIoT_Communication_2018_08_29.pdf (link as of 15/01/2020)
3. Worldwide Internet of Things Spending Guide. IDC. https://www.idc.com/getdoc.jsp?containerId=IDC_P29475 (link as of 15/01/2020)
4. 2019. IDC Forecasts Worldwide Spending on the Internet of Things to Reach $745 Billion in 2019, Led by the Manufacturing, Consumer, Transportation, and Utilities Sectors. IDC. https://www.idc.com/getdoc.jsp?containerId=prUS44596319 (link as of 15/01/2020)
5. World Economic Forum. 2019. 3 ways AI will change the nature of cyber attacks. https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/ (link as of 15/01/2020)
6. World Economic Forum. 2018. Industrial Internet of Things: Safety and Security Protocol. https://www.weforum.org/whitepapers/industrial-internet-of-things-safety-and-security-protocol (link as of 15/01/2020)
7. Critical infrastructure sectors. CISA. https://www.cisa.gov/critical-infrastructure-sectors (link as of 15/01/2020)
8. 2018. Implementation of the NIS Directive DfT Guidance version 1.1. UK Department for Transport. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/765786/implementation-of-the-nis-directive-dft-guidance.pdf (link as of 15/01/2020)
9. 2019. Aviation Cyber Security. IATA. https://www.iata.org/contentassets/e55ae27b2fc34343a1143fca5129c8dd/aviation-cyber-security-position.pdf (link as of 15/01/2020)
10. Cooper, Pete. 2017. Aviation Cybersecurity. Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2017/11/Aviation_Cybersecurity_web_1107.pdf (link as of 15/01/2020)
11. 2016. Cyber-Attack Against Ukrainian Critical Infrastructure. CISA https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01 (link as of 15/01/2020)
12. 2019. Aviation Cyber Security. IATA. https://www.iata.org/contentassets/e55ae27b2fc34343a1143fca5129c8dd/aviation-cyber-security-position.pdf (link as of 15/01/2020)
13. World Economic Forum. Building Cyber Resilience in the Aviation Sector. https://www.weforum.org/projects/building-cyber-resilience-in-the-aviation-sector (link as of 15/01/2020)
14. World Economic Forum. Global Risks Report 2019. https://www.weforum.org/reports/the-global-risks-report-2019 (link as of 15/01/2020)
15. 2019. Aviation Cyber Security Market: Increasing Rate of Cyber-attacks in Aviation Sector. Business Wire. https://www.businesswire.com/news/home/20190802005183/en/Aviation-Cyber-Security-Market-Increasing-Rate-Cyber-attacks (link as of 15/01/2020)
16. Cyber Threat Source Descriptions. CISA. https://www.us-cert.gov/ics/content/cyber-threat-source-descriptions (link as of 15/01/2020)
17. Palmer, Matt. 2018. Recent nation state cyberattacks: What they mean, and how to respond. https://www.willistowerswatson.com/en-US/Insights/2018/04/recent-nation-state-cyberattacks-what-they-mean-and-how-to-respond (link as of 15/01/2020)

18. Europol. Internet Organized Crime Threat Assessment (IOCTA) 2019. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019 (link as of 15/01/2020)

19. 2019. The Cybersecurity Imperative Pulse Report. Willis Towers Watson. https://www.willistowerswatson.com/en-US/Insights/2019/08/the-cybersecurity-imperative-pulse-report (link as of 15/01/2020)

20. World Economic Forum. 2016. Understanding Systemic Cyber Risk. https://www.weforum.org/whitepapers/understanding-systemic-cyber-risk (link as of 15/01/2020)

21. 2018. 87% of Firms see Untrained Staff as Greatest Cyber Risk, According to Willis Towers Watson and ESI ThoughtLab. Globalnewswire. https://www.globenewswire.com/news-release/2018/10/16/1621725/0/en/87-of-Firms-see-Untrained-Staff-as-Greatest-Cyber-Risk-According-to-Willis-Towers-Watson-and-ESI-ThoughtLab.html (link as of 15/01/2020)

22. Computer Security Research Center. NIST. https://csrc.nist.gov/glossary/term/vulnerability (link as of 15/01/2020)

23. Decode cyber risk. Willis Towers Watson Cyber Risk Culture Survey. https://www.willistowerswatson.com/assets/23440/cyber-risk-culture-survey.pdf (link as of 15/01/2020)

24. 2012. Guide for Conducting Risk Assessments. Computer Security Research Center. NIST. https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final (link as of 15/01/2020)

25. ISO/IEC 27005:2018 [ISO/IEC 27005:2018]. ISO. https://www.iso.org/standard/75281.html (link as of 15/01/2020)

26. Cybersecurity Framework. NIST. https://www.nist.gov/cyberframework (link as of 15/01/2020)

27. ISO/IEC 27001 Information security management. ISO. https://www.iso.org/isoiec-27001-information-security.html (link as of 15/01/2020)

28. NCSC CAF guidance. UK NCSC. https://www.ncsc.gov.uk/collection/caf (link as of 15/01/2020)

29. World Economic Forum. 2019. The Cybersecurity Guide for Leaders in Today's Digital World. https://www.weforum.org/reports/the-cybersecurity-guide-for-leaders-in-today-s-digital-world (link as of 15/01/2020)

30. 2019. Aviation Cybersecurity Strategy. ICAO. https://www.icao.int/cybersecurity/documents/aviation%20cybersecurity%20strategy.en.pdf (link as of 15/01/2020)

31. World Economic Forum. 2017. Advancing Cyber Resilience: Principles and Tools for Boards. https://www.weforum.org/whitepapers/advancing-cyber-resilience-principles-and-tools-for-boards (link as of 15/01/2020)

32. 2018. Decode resiliency. Willis Towers Watson. https://eiuperspectives.economist.com/sites/default/files/EIU_WTW%20-%20How%20boards%20can%20lead%20the%20cyber-resilient%20organisation.pdf (link as of 15/01/2020)

33. 2019. Life Inside the Perimeter. Nominet. https://media.nominet.uk/wp-content/uploads/2019/02/12130924/Nominet-Cyber_CISO-report_FINAL-130219.pdf (link as of 15/01/2020)

34. Hietala, Jim. 2017. What is open fair?. The Open Group. https://blog.opengroup.org/2017/01/24/what-is-open-fair/ (link as of 15/01/2020)

35. Quantitative Techniques in Information Risk Analysis. Information Security Forum. https://www.securityforum.org/research/quantitative-information-risk-analysis/ (link as of 15/01/2020)

36. Cyber Quantified. Willis Towers Watson. http://www.willis.com/CoreAnalytics/cyber.html (link as of 15/01/2020)

37. Operational Technology. Gartner. https://www.gartner.com/en/information-technology/glossary/operational-technology-ot (link as of 15/01/2020)

38. 2018. Industrial Networking Enabling IIoT Communication. Industrial Internet Consortium. https://www.iiconsortium.org/pdf/Industrial_Networking_Enabling_IIoT_Communication_2018_08_29.pdf (link as of 15/01/2020)

39. Cyber Threat Source Descriptions. CISA. https://www.us-cert.gov/ics/content/cyber-threat-source-descriptions (link as of 15/01/2020)

40. World Economic Forum. 2016. Understanding Systemic Cyber Risk. https://www.weforum.org/whitepapers/understanding-systemic-cyber-risk (link as of 15/01/2020)

41. Computer Security Research Center. NIST. https://csrc.nist.gov/glossary/term/vulnerability (link as of 15/01/2020)

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744

contact@weforum.org
www.weforum.org