In collaboration
with Deloitte

Pathways Towards a Cyber Resilient Aviation Industry

INSIGHT REPORT

APRIL 2021

Images: Getty Images

Contents

Foreword 3

Preface 4

Executive summary 5

1 State of play in the COVID-19 era 6

1.1 Evolving risk profile and cyberthreat landscape 7

1.2 Taking stock of key industry initiatives 9

2 Barriers to increasing cyber resilience across the industry 10

2.1 Underinvestment in cyber resilience capabilities 11

2.2 Increased complexity of the value chain with ambiguous accountability 12

2.3 Fragmented approach at governance and policy levels 13

2.4 Lack of visibility and transparency across the supply chain 14

3 Recommended pathways towards cyber resilience 15

3.1 Recommendations at international level 17

3.2 Recommendations at national level 21

3.3 Recommendations at organizational level 22

Conclusion 25

Appendix 26

Glossary 28

Acknowledgements 29

Contributors 31

Endnotes 32

Foreword

Fang Liu
Secretary General,
International Civil
Aviation Organization

The International Civil Aviation Organization (ICAO) has been at the forefront of addressing cyberthreats to civil aviation since 2005. We've led the development of International Standards and Recommended Practices and guidance material, supported the adoption of several important international declarations, supported our Member States in their formalizing of two ICAO Assembly Resolutions, and developed an Aviation Cybersecurity Strategy and Action Plan.

The Aviation Cybersecurity Strategy and Action Plan constitutes a comprehensive framework that permits states and stakeholders to collaborate more efficiently as they refine a global, robust and holistic approach to cybersecurity and cyber resilience across civil aviation domains.

The work of the World Economic Forum on aviation cyber resilience complements these global efforts led by the ICAO and is another excellent example of the importance of broad-based international collaboration among public and private stakeholders.

ICAO is pleased to contribute to this report, which highlights the continuous cooperation between our organization and the Forum. We also look forward to fostering cooperation and collaboration between all stakeholders in addressing this important topic to assure the continued safety, security, efficiency and sustainability of the global civil aviation sector.

Eamonn Brennan
Director General,
EUROCONTROL

The aviation industry is increasingly digital, but the COVID-19 pandemic having decimated our industry over the past year means there are far fewer funds available for investments in cyber resilience. Cybercriminals have already been able to take advantage of this weakness. We are delighted to have contributed to this World Economic Forum initiative to support the aviation industry to become more cyber resilient and able to resist the cyberthreats of today and tomorrow.

Patrick Ky
Executive Director,
European Aviation
Safety Agency

The global civil aviation ecosystem is accelerating towards more digitalization. This implies that any exchange of information within any digital workflow of the aviation community needs to be resilient to information security threats which have consequences on the safety of flight or the availability of airspace and beyond. The European Union Aviation Safety Agency (EASA) is transforming itself to embrace such digitalization by designing new digital workflows (e.g. for the issuance of licenses, approvals and certifications), in consultation with the worldwide aviation community, and the European Strategic Coordination Platform (ESCP). It is also developing new EU rules to address information security risks in a comprehensive and standardized manner across all aviation domains. To underline EASA's commitment, its related activities are documented in the agency's work plan and performed in coordination with its participating states.

Nick Careen
Senior Vice-President
Airport, Cargo, Passenger
and Security, International
Air Transport Association

2020 was a devastating year. The pandemic brought the aviation industry to a dead stop but had the opposite impact on cybercrime. Many experts reported the rise of cyberattacks during this period. This upward trend calls for unprecedented actions to tackle and build resilience for corporate and interconnected systems. Collaboration is our greatest protective measure and I hope that this report will trigger the necessary discussions and actions towards building our cyber resilience in this evolving technological ecosystem.

Preface

Georges de Moura
Head of Industry Solutions, Centre for Cybersecurity, World Economic Forum

Lauren Uppink
Head of Aviation, Travel and Tourism Industries, World Economic Forum

Geoff Wylde
Lead, Internet of Things and Urban Transformation

Chris Verdonck
Partner, Deloitte, Belgium

The aviation industry has long been lauded for its impeccable safety record, demonstrating that with global cooperation, standards and governance, an industry can work together to ensure the utmost responsibility for and safety of its personnel and its customers.

The Fourth Industrial Revolution – fuelled by the proliferation of sensors and embedded computing systems (the "internet of things") – has enabled a convergence of information technology (IT) and operational technology (OT). As disparate parts of our complex infrastructure and industrial ecosystems are digitally connected, new levels of speed, productivity and collaboration are introduced, hidden and complex risks also emerge.

Digital transformation alongside the exponential growth of the aviation industry has made for an increased threat surface which must be urgently addressed. To harness this opportunity and mitigate potential risks, society must reimagine how we use and manage our critical infrastructure. This involves understanding how our individual actions impact the collective and establishing frameworks for shared responsibility.

Despite the significant knock the sector has faced from the COVID-19 pandemic, it remains one of the most crucial in terms of providing access to economic and social benefits. As the world grows ever more complex, the industry must guard against growing numbers and varieties of threats.

The World Economic Forum continues to work with its aviation stakeholders to ensure that the benefits of aviation will become increasingly accessible across the world, and this cannot be done without ensuring its long-term resilience and sustainability. To do this, all manner of risks must be anticipated and mitigated, whether it be physical, climate related or cyber in nature.

With this in mind, the Forum collaborated with Deloitte and a multistakeholder community to advance cyber resilience in the aviation sector and help identify, measure and shape approaches to mitigate cyber risks that are endemic to technology adoption in our critical infrastructure. This body of work has served as a jumping-off point for continued collaboration within the aviation community but also as a model for other industries and ecosystems to build upon.

This report is a meaningful step towards aligning the interests and actions of the aviation security community to ensure that cybersecurity is embedded into the strategies of all aviation businesses as it recovers and rebuilds after the devastating effects of the pandemic. Without the previously experienced pressure of a rapidly growing industry, the pandemic, as hard-hitting as it has been, provides the aviation industry with a window of opportunity to redesign its systems to be future-proof and hardy in the face of yet another crisis.

Executive summary

Cyber resilience in the aviation industry will be strengthened through global collaboration and multistakeholder mobilization.

Air transport is a vital industry that contributes substantially to economic development and the improvement of living standards. The role of the aviation industry in commerce, trade and transport infrastructure makes it indispensable to the global economy. The consequences of any major technological or organizational failure carry direct public safety and national security implications and costs.

As international travel almost came to a complete standstill in 2020 due to the COVID-19 pandemic, the aviation industry suffered a catastrophic year. Global passenger traffic declined 65.9% compared to 2019. International passenger demand dropped 75.6% and domestic demand fell 48.8% below 2019 levels. In 2021 the aviation sector will play a vital role transporting vaccines – the largest single transport challenge in its history. It is highly likely that aviation networks and other sectors associated with the vaccine distribution supply chain will be subject to a significant volume of targeted, adversarial cyber activities during this high-profile campaign.[1]

The COVID-19 pandemic is the latest reminder that both the frequency and severity of catastrophic shocks have increased in recent times, and that building greater resilience in the future has become a defining mandate of our era. According to the World Economic Forum's *Global Risks Report 2021*,[2] cybersecurity failure and tech governance failure are among the top mid-term global threats. Our increased reliance on digital infrastructure and the rapid adoption of emerging technologies has further exacerbated vulnerabilities and increased the inequalities in governance practices between countries, industries and businesses.

To ensure the aviation industry can better navigate future shocks, the development of two concurrent resilience strategies will be critical – both at corporate and ecosystem-wide levels. Aviation organizations would need to:

- consider cyber risks in the broader context of corporate and the ecosystem's resilience, looking at both the cyber and physical elements of operational risks to their business as they become increasingly dependent on the internet and digital channels

- adopt a resilience mindset to govern how they would respond to and recover from any major cyber event as an extension to their robust emergency response practices for safety and physical security incidents

The World Economic Forum's Cyber Resilience: Aviation community, comprised of senior cybersecurity leaders from the aviation industry ecosystem, government agencies and international organizations created this report to highlight key systemic cyber risks, and to prioritize and define pathways to anticipate and mitigate the impact from future digital shocks.

This report is a call to action for business leaders, regulators and policy-makers, cybersecurity practitioners and technology providers. It aims to define a common language to encourage collective initiatives for increasing cyber resilience across the ecosystem. A first step is establishing an inclusive framework that can adapt to the different regulatory requirements of the wide variety of actors involved in the aviation ecosystem. It must simultaneously uphold a strong security baseline, fit to ensure safe and secure travel. The benchmarking exercise in this initiative will increase the visibility and transparency of cyber risk management and governance practices across the aviation digital ecosystem and can lead the way to further improvements.

1 State of play in the COVID-19 era

As the world emerges from the pandemic, cyber security must remain a priority to protect aviation's most critical assets.

Cyber resilience can be defined as: “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources”.[3]

The effect of COVID-19 on civil aviation can hardly be understated. In January 2021 the European Organisation for the Safety of Air Navigation (EUROCONTROL) recorded a 64% drop in civil flights in its network of 41 member states compared to pre-pandemic figures. The US and the Middle East similarly recorded a drop of 45% and 57% in international flights respectively.

As a result of a sudden and lasting drop in revenue, funding and resources allocations are constantly reprioritized to enable business continuity. The large-scale adoption of remote-access technologies to enable work-from-home practices, with greater reliance on digital services, enabled companies to continue operations and reduce costs in conditions of social distancing and stay-at-home orders from government and/or employer. It is also reshaping the digital landscape and architecture while straining supply chain resiliency and cybersecurity operations with the escalating risk.[4]

A combination of external factors is likely to impact critical functions of the aviation industry ecosystem, including its cyber resilience. Figure 1 highlights potential threats to the global aviation ecosystem’s cyber resilience.

FIGURE 1 **Impact of the COVID-19 pandemic on the aviation industry**

Working from home	Fast rising social engineering attacks	Ambiguous accountability in supply chains	Rapid innovation	Critical infrastructure services
Heightened dependency on mobile (personal) devices and residential networks increases the attack surface	Malicious actors use increasingly sophisticated social engineering tactics on a distracted and vulnerable workforce	As supply chains increase in complexity, a lack of oversight and ambiguous accountability impact cyber resilience	Rapid digitalization may lead to organizations bypassing risk assurance steps, changing the risk profile potentially to an unknown state	Critical infrastructure services remain under acute pressure and are particularly targeted by sophisticated attacks led by criminal organizations and nation state actors

1.1 Evolving risk profile and cyberthreat landscape

As deeper performance insights and new levels of connectivity allow businesses to reap the benefits of breakthrough technologies, the world is becoming faster, more flexible and more efficient. This shift is creating a global ecosystem where physical and digital entities are increasingly connected, from critical infrastructure assets to people and data. These risks highlight the need for a common understanding and common approach towards existing and emerging threats to enable industry and government actors to implement appropriate countermeasures to mitigate supply chain security risks.

Revenues and cyber budgets are dwindling, cyberattacks are not. The sudden change in our way of working, combined with the sense of urgency and uncertainty generated by the COVID-19 pandemic, proves to be fertile ground for cybercriminals and nation-state actors.

Phishing is still one of the most common attack vectors and there has been a surge in COVID-19 related scams. In a survey conducted in 2020 by Airports Council International (ACI), 87.2% of respondents named social engineering as their greatest vector of compromise.[5] Additionally, phishing emails that focus on specific targets – such as chief executive officers, financial departments and procurement teams – have increased in sophistication.

Ransomware activities targeting businesses skyrocketed over the past two years, with a 365% increase in detections in 2019.[6] Other targets include critical infrastructure providers, such as hospitals, power utilities and airports. Loss of life has occurred as an indirect result. In addition, such attacks on hospitals can harm public trust and cause significant economic and reputational damage.

In February 2021 a major information technology company providing airline-passenger service systems confirmed being hit by a highly sophisticated cyberattack. Supplying IT systems for around 90% of the global aviation industry, the firm stated that its US servers were compromised.[7]

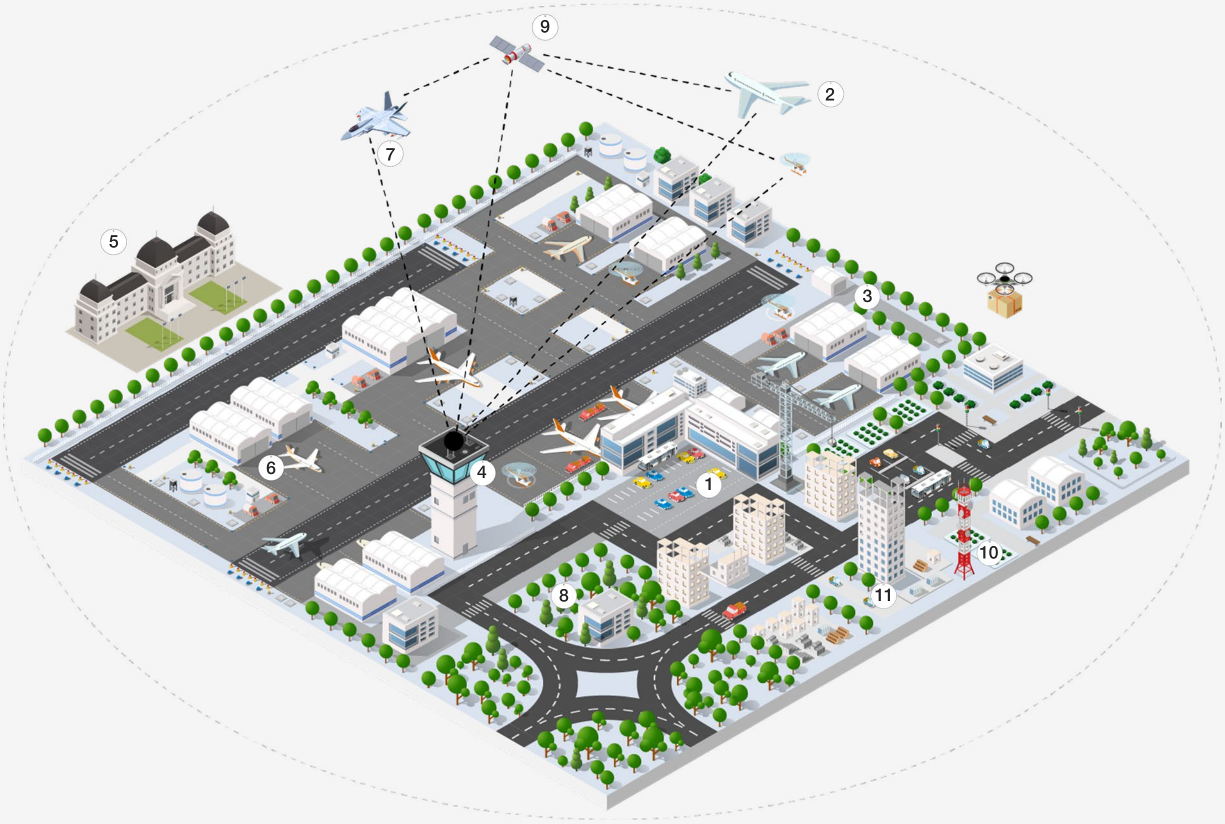
The complete impact of the attack is not yet known, however, millions of passengers are expected to be affected. Based on available data, the attack points to a concerted effort to target global supply chains associated with providers of critical infrastructure.

COVID-19 vaccine distribution

National defence, vital emergency services and critical infrastructure rely heavily on the aviation industry and expect it to shift gears swiftly. The role of aviation in distributing COVID-19 vaccines perfectly illustrates the need for flexibility and resilience. Adjusting to the scope and scale of delivering COVID-19 vaccine requires an accurate assessment of available temperature-controlled facilities. It demands enough qualified personnel to monitor capabilities and guarantee vaccine integrity. In addition, existing security protocols must be scaled up to protect the valuable commodity from theft and potential tampering. All processes rely on adequate and reliable data-sharing.

Apart from actors traditionally linked to the aviation industry – such as airlines, airports, aircraft manufacturers and air navigation service providers – the aviation ecosystem also includes less visible actors. Through acquisitions and partnerships, actors usually associated with other industries play an integral role in the broader value and supply chains of the aviation ecosystem.

FIGURE 2 The breadth and complexity of the aviation ecosystem



Ecosystem actors

1 Airports
2 Airlines
3 Engineering and maintenance
4 ANSP
5 Government agencies
6 Manufacturing
7 Military aviation
8 Travel agencies
9 Satellite providers
10 Telecom providers
11 IT-OT providers

Source: Deloitte

1.2 Taking stock of key industry initiatives

In an industry where unaddressed risks could have major implications for the safety of individuals, as well as reputational and financial losses for organizations, the need for a systemic approach to cyber risk has long been identified. The Assembly of the International Civil Aviation Organization (ICAO) has recognized the need to boost resilience to cyberthreats on a global scale and has identified actions to be taken by states and other stakeholders. The ICAO's efforts include calls to action to national governments in the form of Assembly Resolutions (A39-19 in 2016 and A40-10 in 2019), an Aviation Cybersecurity Strategy (2019), a Cybersecurity Action Plan (2020) and a Training Roadmap (2020). Simultaneously, with the establishment of a multidisciplinary Trust Framework Study Group (TFSG), the ICAO is developing a trust framework to support information exchange in a global, digitally connected environment. The TFSG's core objective is to reduce the cyberattack surface and improve cyber resilience for a digitally connected aviation ecosystem.

Cybersecurity Action Plan

ICAO-identified actions for achieving a cyber-resilient aviation ecosystem:

- recognize the necessity of developing a comprehensive and agreed upon cybersecurity vision as a solid foundation for coordinated, global cybersecurity risk management
- work towards a common baseline for cybersecurity standards and recommended practices
- ensure that cybersecurity is part of aviation security and safety systems, and a comprehensive risk-management framework
- ensure a variety of risk-assessment methodologies to ensure comparability
- develop information-sharing platforms and mechanisms in line with existing ICAO provisions, to allow prevention, early detection and mitigation of relevant cybersecurity events
- ensure the qualification of personnel in both aviation and cybersecurity
- increase awareness about cybersecurity

Developed in collaboration with national regulators, industry associations and other key stakeholders, the Action Plan will drive greater international alignment on cyber risk management practices and cybersecurity regulations.

Trust Framework Study Group (TFSG)

The ICAO's TFSG aims to connect international organizations and relevant stakeholders to urgently and transparently develop a globally harmonized aviation trust framework.

The TFSG focuses on four operational areas:

- digital identity management
- network security
- performance
- resilience requirements

Industry associations – the International Air Transport Association (IATA), the Airports Council International (ACI) and the International Coordinating Council of Aerospace Industries Associations (ICCAIA), among others – support and promote cyber resilience by disseminating guidance, training materials and tools. Trade associations actively engage and participate in developing international regulations with organizations such as ICAO and the European Union Aviation Safety Agency (EASA). In line with the ICAO Aviation Cybersecurity Strategy, industry associations and industry leaders have created several groups to foster knowledge sharing, including risk information. In response to the COVID-19 pandemic specifically, IATA supported the industry by recommending cybersecurity practices for prolonged aircraft storage, and in collaboration with the Aviation Information Sharing and Analysis Centre (A-ISAC), for vaccine distribution and possible disruption of the cargo supply chain by malicious actors. Still, these initiatives are fragmented. More needs to be done to build communities and collaboration between actors with varying activities.

“ **ICAO's vision for global cybersecurity is that the civil aviation sector is resilient to cyberattacks and remains safe and trusted globally, whilst continuing to innovate and grow.**[8]

2

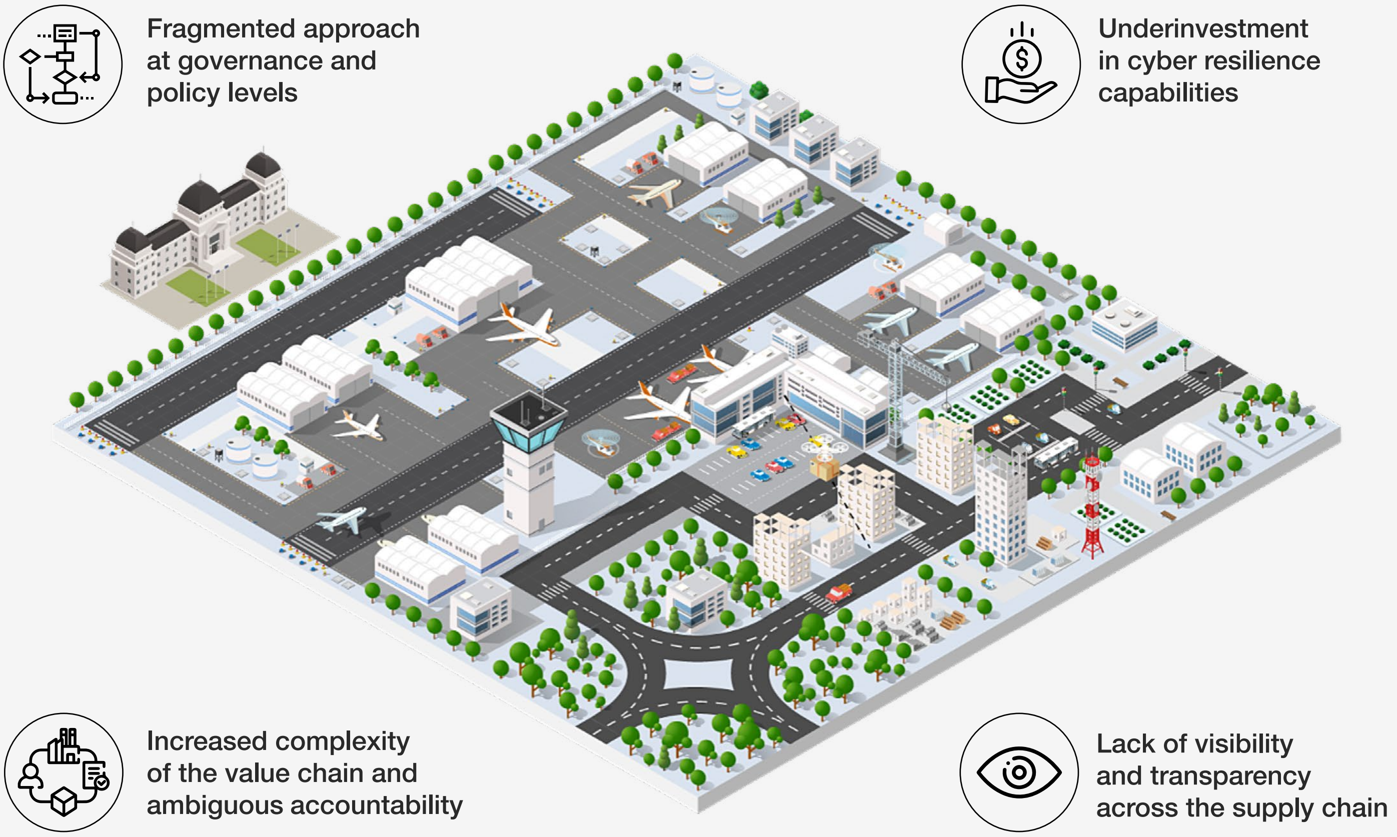
Barriers to increasing cyber resilience across the industry

Although aviation stakeholders are determined to achieve higher cyber resilience levels, their efforts are hindered by various organizational, technical and regulatory barriers.

Although aviation stakeholders are determined to achieve higher cyber resilience levels, their efforts are hindered by various organizational, technical and regulatory barriers. Overcoming these barriers will require a holistic, systematic and collaborative approach by multiple stakeholders in the public and private sector.

Businesses, governments and civil societies have already spearheaded many initiatives to build cyber resilience, but they are limited in scope, often isolated and disconnected. To ensure better international alignment and coordination of strategic efforts in the area of cyber resilience, the ICAO established the Secretariat Study Group on Cybersecurity in 2017. It then developed the Aviation Cybersecurity Strategy for the civil aviation sector, as well as a Cybersecurity Action Plan to help states and stakeholders implement the strategy (in 2019[9] and 2020 respectively). The Group also provides a forum for states and concerned stakeholders to globally harmonize the aviation sector's approach to cybersecurity and cyber resilience.

FIGURE 3 Barriers to cybersecurity and cyber resilience


Fragmented approach at governance and policy levels
Underinvestment in cyber resilience capabilities
Increased complexity of the value chain and ambiguous accountability
Lack of visibility and transparency across the supply chain

Source: Deloitte

2.1 Underinvestment in cyber resilience capabilities

The COVID-19 pandemic has created an unprecedented existential crisis for the aviation sector. As restrictions continue, the prolonged decline in air travel demand has impelled aviation organizations to maintain a minimum operational level and reprioritize their investments and resources to "keep the lights on".

The rapid transition to remote working, workforce downsizing and changes in operating models have increased the need for greater vigilance and attention to adversarial cyber activities. Aviation businesses are faced with a dilemma: while exposure to cyberattacks remain high with a broader, more complex and more complicated attack surface, their ability to fund and resource cybersecurity defence has come under tremendous pressure. These businesses have to strike a delicate balance between operational, financial and cybersecurity risks to achieve long-term growth, prosperity and resilience for their organization and industry.

The high success rate of social-engineering scams such as phishing reveals a growing divide: between increased sophistication and attack capabilities on one side, and low cyber literacy of employees and lack of defence capabilities on the other. This presents a major risk for organizations.

Cost-saving and accelerated technology implementation have enabled operational continuity, but also brought new risks. Such rapid digital transformation can lead to insufficient attention to cybersecurity, as defence is regarded as a non-essential component.

Figure 3 (previous page) illustrates that a proactive implementation of controls will, in the long term, be more beneficial when an adverse event occurs. Rushed technological implementations and budgetary restraints, however, may tempt organizations to take a reactive stance towards cyber resilience. As the digital ecosystem continues to transform, the accumulated technical deficit and security risks will become increasingly difficult and costly to manage – even more so if cyber resilience is regarded as a retroactive consideration. Without continuous investment and commitment to cyber resilience, organizations will be more vulnerable to cyberattacks and thus more likely to endure reputational, financial, operational and safety impacts.

2.2 Increased complexity of the value chain with ambiguous accountability

The aviation ecosystem is characterized by a high level of interconnectivity and interdependence. Each actor, direct or indirect, plays an important role: supplying products, operating and integrating them, and maintaining the system as a whole, as well as its sub-systems. Therefore, the aviation industry is often referred to as a "system of systems" (SoS).[10]

In most cases, the industry's different sub-systems were designed, integrated, operated and managed by different organizations independently of each other, and evolved at their own pace without a clear understanding of the whole architecture. Different systems must be capable of working autonomously, while ensuring interoperability and integration with all interconnected systems to maintain efficient operation and overall cyber resilience.

> “ The high success rate of social engineering scams such as phishing reveals a growing divide: between increased sophistication and attack capabilities on one side, and low cyber literacy of employees and lack of defence capabilities on the other.

This leads to ambiguous accountability. As supply and value chains become more complex, measures must also evolve beyond securing individual systems. A static approach will not suffice; industry players need to address their individual, as well as shared responsibilities to secure the ecosystem.

Harnessing emerging technologies brings tremendous potential: more operational efficiency, better data-driven decisions, and better overall customer experience and satisfaction. With these great technologies comes greater risks, too. Physical and digital entities are becoming increasingly connected – from critical infrastructure assets, to people and data, to technologies that include biometrics, artificial intelligence (AI), machine learning and the Internet of Things (IoT). Increased digitalization of aviation and information systems is also continuing at pace, as the sector seeks to increase airspace capacity and throughput.[11]

As highlighted in the World Economic Forum's report of November 2020: *Future Series: Cybersecurity, emerging technology and systemic risk,* the increased complexity, pace, scale and the interdependence of technological trends overwhelm the current cyber defences of enterprises. The report urges business leaders to plan more strategically for emerging risk so they can ensure that the organizations delivering the most critical infrastructures do not suffer failures that are catastrophic for societies.[12]

At the cutting edge of this issue is the ICAO Trust Framework Study Group (TFSG). The TFSG aims to securely and digitally connect aviation assets and units around the globe to facilitate information-sharing for multiple purposes, including real-time traffic management. Airports are also increasingly connected and digitized, with many services having remote or wireless connections, including access-control and airside systems, such as maintenance, tugs and high-speed wireless between aircraft and docking gate. All of these digitized services exist against a backdrop of complex airport management and accountability, making it difficult to holistically define and defend an attack surface.

Many such services — spanning aircraft, ATM and airport — increasingly rely on space-based assets for their operations, which range from data transfer and communications to positioning, navigation and timing (PNT).[13] As legacy and analogue systems are replaced by space-based capabilities, their cybersecurity and resilience must increasingly be scrutinized.

The use of 5G networks is also expected to rapidly grow across the aviation sector. In 2021 the estimated 5G market in aviation will be worth $500 million, with projected growth to $3.9 billion by 2026. 5G will likely become a ubiquitous means of communication across every aspect of the aviation sector, with advantages based on size (connectivity at 'chip level'), low-power requirements and flexibility. But 5G prevents several cybersecurity challenges. The European Network and Information Security Cooperation group asserts that: “5G will increase the overall attack surface and the number of potential entry points for attackers”, alongside the challenge of third-party supplier risk management.

Overall, the difficulty of understanding risk across interdependent and complex digitalized aviation systems with extensive supply chains is only increasing. Securing the supply and value chains must address the end-to-end product life cycle, including design, commission and operations until decommissioning. The different entities in the supply and value chain must collaborate on business-critical activities for products and systems, and hence an isolated approach will not suffice. A resilient ecosystem requires individual as well as shared responsibilities.[14]

2.3 Fragmented approach at governance and policy levels

Existing practices of information security management systems and corporate governance are inherently limited to individual organizations. This means that governing and managing cybersecurity and its related risks are often not performed beyond the perimeter of the organization.

Approaching cyber security from an isolated-perimeter-perspective is insufficient to counter the risks introduced by the System-of-Systems architecture. It can lead to blind spots and a misunderstanding of residual risks from interconnection points in the supply and value chains, compounded with ambiguous accountability related to cyber resilience. A collaborative approach from all actors in the aviation value chain should be leveraged, building on a strong history of safety management systems and cross-sector safety collaboration. This will help ensure that cyber risks are adequately and consistently governed and managed across the aviation digital ecosystem.

National or regional cybersecurity strategies, regulations and policy frameworks (such as the European Directive on Security of Network and Information Systems or “NIS Directive”) recognize that the market alone cannot effectively incentivize appropriate cybersecurity practices, particularly for critical infrastructure where a cyberattack can affect critical functions.

The fragmented regulatory landscape however poses a barrier to aligning approaches nationally and internationally. The NIS Directive, for instance, is interpreted, implemented and enforced separately by each European Union Member State, leading to wide disparity in laws and regulations. Additionally, the assurance frameworks and processes for verifying compliance are limited, with audits and inspections occurring very infrequently and fines imposed only in the most egregious cases. Often regulators do not have the legal authority to impose a fine. Under the NIS Directive, each country has discretion about when to impose a fine and its amount, if the minimum requirements are clearly established. Some of these regulatory gaps are being addressed in the revised European NIS Directive, scheduled for a vote in 2021.

“ A collaborative approach from all actors in the aviation value chain should be leveraged, building on a strong history of safety management systems and cross-sector safety collaboration.

The revised NIS directive will cover four key areas: 1) greater capabilities for supervision and sanctions by national authorities, 2) use of EU certification schemes and integration with network codes, 3) increased cooperation for crises, incidents and information sharing, and 4) alignment of cyber risk management requirements.

These national cybersecurity strategies and regulations would cover critical infrastructure industries such as transportation. However, the diversity of the industry ecosystem makes it difficult to regulate each sector at a national level, when capacity and skilled workforces are limited in most national cybersecurity agencies. Emerging countries especially lack plans to establish national cybersecurity agencies. Besides, for the aviation industry, the regulation and minimum standards would often derive from those defined for the transportation sector.

The power of international and government organizations – such as the European Aviation Safety Agency (EASA), and national civil aviation authorities (CAAs) like the Federal Aviation Administration (FAA) in the US – are limited by their mandate. Meanwhile, neither digital innovation nor cyberthreats are waiting for regulators to take action.

Better interoperability at technical and policy level will help realize the potential value of securing the global digital ecosystem. Collaboration between actors is a necessary step to ensuring sustainable, systemic resilience. Currently, many cyber resilience initiatives have emerged on strategic, tactical and operational levels within the industry, but they tend to be fragmented and limited in scope.

2.4 Lack of visibility and transparency across the supply chain

There is a general consensus that access to timely and actionable threat intelligence would improve a company’s security, however, such information-sharing between industry actors and government agencies is rare and is hindered by the lack of effective and common data-sharing mechanisms and models.

Sharing different types of data requires appropriate security and privacy controls and mechanisms, depending on how critical it is. For example, the sharing of publicly known vulnerabilities and best practices would never be handled in the same way as a company’s private assessment results, or as intelligence related to an incident.

Besides, complex and dynamic data privacy and national security laws need to be taken into account not only within an organization, but also beyond. This raises concerns about legal liability and reputational damage if the wrong information is shared.

There must be increased dialogue and contributions from all aviation-sector stakeholders, including manufacturers, end users, governments and regulators. There is also a risk that the disclosure of actionable insights will become increasingly limited, when there should be an increase in transparency and collaboration. To overcome these challenges, partnerships must develop between all stakeholders that focus on minimizing risk, rather than legal jeopardy.[15]

3

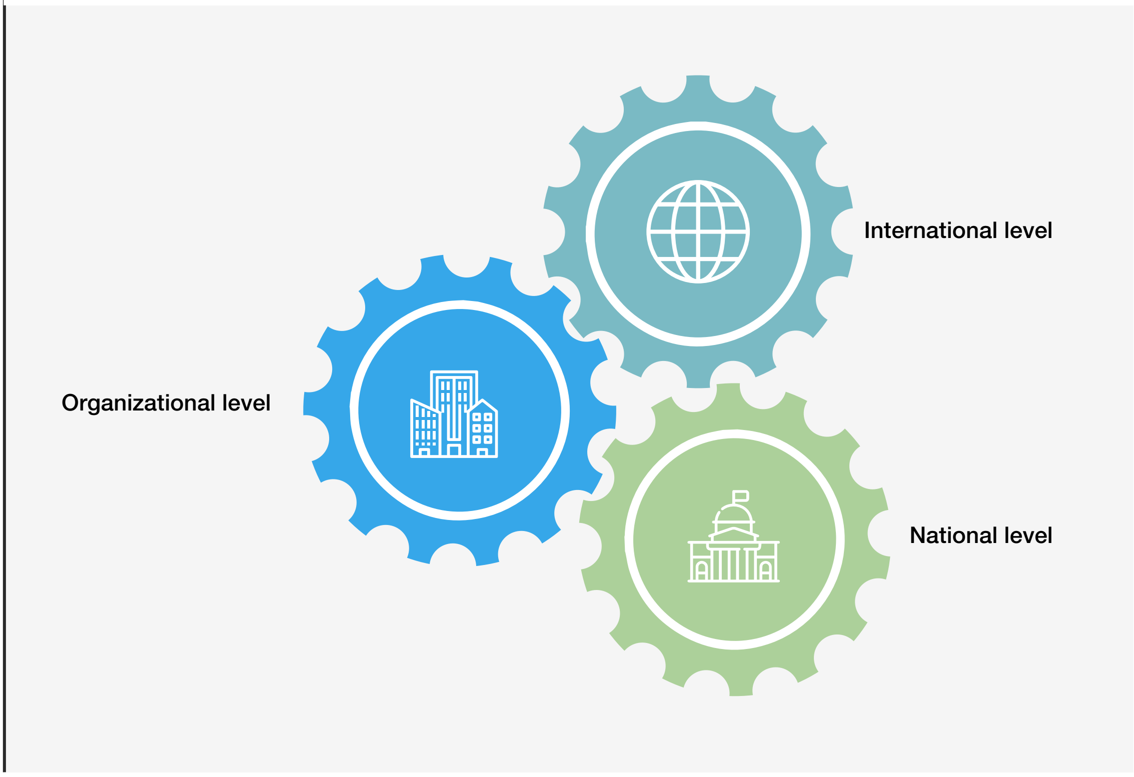
Recommended pathways towards cyber resilience

To address barriers and challenges to cyber security, decisive and collective action is required on three levels: international, national and organizational.

Barriers to increasing cyber resilience in the aviation ecosystem have always existed and always will. The COVID-19 pandemic has intensified some of these barriers and made it difficult for businesses to dedicate time, money and resources to overcome them. Most of the efforts in the past year were focused on crisis management and "keeping the lights on". Now the time is ripe for aviation businesses to take decisive action to tackle some of these barriers and challenges head on.

This report includes recommendations on three levels: international, national and organizational, each sphere has its own tools and limits on what it can achieve. To move forward, stakeholders at all levels must work together, anticipating gaps and building on each other's strengths.

FIGURE 4 Recommended three levels of action



3.1 Recommendations at international level

FIGURE 5 International level

International level

– Aligning regulations globally
– Establishing a cyber resilience baseline
– Encouraging continuous assessments and industry benchmarking
– Developing information-sharing frameworks and standards

Aligning regulations globally with balanced and outcome-based guidance

Regulating civil aviation requires an international approach to ensure the safety, security, trade and commercial usage of airspace, and that environmental impacts are adequately addressed. The fast-paced digital transformation of the aviation industry has complicated the creation of fit-for-purpose regulations.

The International Civil Aviation Organization (ICAO) is the main supranational agency developing standards and recommended practices concerning safety, air navigation, infrastructure, flight inspection, prevention of unlawful interference, and facilitation of border-crossing procedures for international civil aviation. Standards and recommended practices (SARPs) adopted by the ICAO tackle highly technical as well as organizational topics. Yet, the subject of cybersecurity and other threats that may arise from increased digitalization is not yet fully covered.

The 39th Session of the ICAO Assembly recognized the need to achieve resilience to cyberthreats on a global scale. In its 40th Assembly Resolution A40-10 – Addressing Cybersecurity in Civil Aviation, the Assembly acknowledged the urgency and importance of protecting civil aviation's critical infrastructure, information and communication technology systems and data against cyberthreats and voiced its commitment to developing a solid cybersecurity framework. The resolution addressed cybersecurity through a horizontal, cross-cutting and functional approach, reaffirming the importance and urgency of protecting civil aviation's critical infrastructure systems and data against cyberthreats, and calls upon Member States to implement the ICAO Cybersecurity Strategy published in 2019.[16] Within the context of this commitment, an Action Plan (2020) and Training Roadmap (2020) were developed, and a multidisciplinary Trust Framework Study Group (TFSG) was established.

The UK model on cyber resilience

The United Kingdom developed a balanced approach to regulating its critical infrastructure sectors, with the UK Civil Aviation Authority mandating that the National Cyber Security Centre's Cyber Assessment Framework (CAF) is referenced. Operators of essential services, including aviation, are required to manage network and system cyber risks in an appropriate and proportionate manner. They are also mandated to implement effective measures to prevent and minimize the impact of related incidents. Operators may be fined, and in some cases, there may be licensing consequences[17]. Such models could serve as a reference for other national regulatory bodies.

Establishing a cyber resilience baseline across the supply and value chains

Regulations and other government instruments will remain critical components of a safe and resilient global aviation industry. Aviation businesses cannot wait, however, for regulations to be developed and enacted as they take time and are unable to keep up with the pace of change.

Historically the aviation industry has had some of the most stringent requirements in physical safety and security. The same principles must now also be applied to cyberspace to safeguard customer data and avoid any harm or disruption to essential functions. As the level of interconnectivity and interdependency rapidly increases, it is no longer sufficient to secure your own organization. The whole supply and value chain needs to be resilient against cyberthreats, as an attack on the weakest link could have cascading effects across the ecosystem.

Furthermore, there is a plethora of best-practice cybersecurity frameworks adopted by organizations, such as ISO 27001/2, NIST, CSF and CIS20, however, there are no universal cyber resilience practices ensuring consistent ways of assessing cyber resilience levels. Such disparity in risk management practices increases the likelihood of blind spots in coverage, especially along the supply chain, as attackers always look to exploit any vulnerabilities. Moreover, the various national regulatory bodies have different security requirements and risk assurance processes, making compliance both complex and burdensome for companies operating globally.

To advance cyber resilience in the aviation ecosystem and better prepare for large-scale and sophisticated attacks, the World Economic Forum provided a platform to foster collaboration through a multistakeholder community with a common purpose. This platform created bridges for public-private and cross-industry collaboration globally. Since early 2020 this community of experts and leaders has been collaborating to strengthen cyber resilience, and to amplify some of the most salient challenges and best practices, as highlighted in the World Economic Forum's 2019 report: *Advancing Cyber Resilience in Aviation: An Industry Analysis*.[18]

One of the actions the report highlights is a common minimum baseline of best practices for cyber resilience that would be applicable for all types of aviation business, regardless of size or geographical location. It highlights a need for greater international alignment of risk management and governance practices. Validated by this community, the Forum's Advancing Cyber Resilience: Principles and Tools for Boards,[19] and the UK's Cyber Assessment Framework (CAF),[20] could serve as valuable references. Combined, these frameworks allow holistic insights into the cyber resilience capabilities of an organization. They are detailed enough to capture the nuances, as well as high-level enough to apply in all geographies and across organizations with varying maturity levels. They are tailored to the industry without being too specific and limited in reach.

UK Civil Aviation Authority's Cyber Assessment Framework for aviation

As part of its work to improve the cybersecurity of critical national infrastructure, the UK National Cyber Security Centre (NCSC) developed and published the Cyber Assessment Framework (CAF), based on four top-level objectives and 14 principles. The CAF was created to meet the following requirements:

- provide a suitable framework to assist in carrying out cybersecurity and resilience assessments
- maintain the outcome-focused approach of NCSC cybersecurity and resilience principles, and discourage box-ticking assessments
- compatibility with appropriate existing cybersecurity guidance and standards
- enable the identification of effective cybersecurity and resilience-improvement activities
- extendibility to accommodate sector-specific elements, as needed
- be able to set meaningful security-level targets for organizations to achieve, possibly reflecting a regulator view of appropriate and proportionate security
- be as straightforward and cost-effective to apply as possible

The Civil Aviation Authority adopted this framework for the aviation sector as it closely supports risk-based oversight principles.[21]

World Economic Forum Advancing Cyber Resilience: Principles and Tools for Boards

The framework aims at cyber resilience strategy and governance, rather than tactics, standards or management. It includes principles leveraged in benchmarking to gauge top management and board-level risk governance practices.[22]

A widespread adoption of these or any other commonly accepted frameworks would be a first step towards reaching a cyber resilience baseline across the aviation industry, which can then be used to further build upon.

Encouraging assessments and industry benchmarking

“ Promoting the adoption of universal risk management practices and the assessment of cyber resilience capabilities increases the visibility into single organizations, as well as the entire value chain.

The digital ecosystem is only as secure as its weakest link. The ever-increasing complexity and interconnectedness of systems makes these weaknesses harder to find. In an environment where organizations struggle to understand their own cybersecurity postures, benchmarking against a common baseline remains essential, yet challenging.

Current risk-assurance practices rely on resource-intensive and laborious mechanisms that are unable to keep up with the scale and pace of change in supply chains. This leaves organizations with increasing unknown residual risks and blind spots that further exacerbate exposure to cyberattacks. Promoting the adoption of universal risk-management practices and the assessment of cyber resilience capabilities increases the visibility into single organizations, as well as the entire value chain. Assessment results can also be used to benchmark across industries and sectors.

In 2020 the World Economic Forum’s Cyber Resilience in Aviation community conducted a benchmarking exercise with a pilot group of aviation stakeholders on a secure online benchmarking platform[23]. Both the Forum’s cyber resilience principles and the UK Cyber Assessment Framework were leveraged for this exercise.

The benchmarking exercise relied on a self-assessment mechanism that is efficient, easy to scale and needs less time and resources than an independent audit, which is important in the resource-constrained context of the COVID-19 pandemic. It proved a great instrument to give organizations insights into their current cyber security posture. The self-assessment approach will enable organizations to assess and monitor their cybersecurity postures, identify strengths and weaknesses, benchmark security performance against an industry baseline, measure the impact of risk-mitigation efforts, and report security progress to boards of directors more clearly and effectively.

Although a self-assessment has certain limitations related to the lack of auditable evidence, using these two frameworks in a global benchmarking pilot is a first step towards reaching a collective understanding of cyber resilience practices across the industry.

Developing international information-sharing frameworks and standards

The distributed nature of many digital ecosystems can make it difficult for a single organization to efficiently identify cyberattacks. Overcoming this problem requires real-time, transparent and actionable information sharing to build collective situational awareness and ensure better preparedness to future adversarial activities.[24]

Sharing information between public and private sector entities and civil organizations – such as EUROCONTROL, Aviation Information Sharing and Analysis Center (Aviation ISAC) or the European Centre for Cybersecurity in Aviation (ECCSA) – will be a crucial next step to get ahead of attackers. Having a consolidated view of potential threats increases the overall situational awareness and enhances the ability of aviation businesses to anticipate cyber adversarial activities and prepare for a potential incident. This also allows organizations to better manage risk and prioritize defences by focusing on pertinent threats. The massive amounts of information being shared between aviation stakeholders raises the need for aviation-tailored data-sharing models and standards.

Collaboration must go beyond subscription to information feeds and include active participation in industry action groups, which should strive to coordinate actions against cybercriminal groups and nation-state actors, thus having a more strategic impact on adversaries by sharing contextual and actionable insights.[25] It should be noted, however, that small and medium-sized businesses might have limited capacity to consume this information and act on these insights.

To tackle this challenge, communities such as the one hosted by the World Economic Forum are closing this gap by fostering public-private collaboration and dialogues that leverage the Forum's independent and impartial platform. Aviation ISAC also plays an important role in facilitating collaboration across the industry by sharing threat-intelligence analysis, and through action-oriented working groups. However, these communities are often membership based, regional, limited to specific aviation stakeholders, and cover only certain use cases.

Existing data-sharing models need to be leveraged for the aviation industry to improve situational awareness and facilitate the sharing of actionable and strategic insights in the face of increasingly complex digital ecosystems. These need to be effective across national boundaries as well as supply chains, recognizing divergent national security and regulatory practices, and must be respectful of personal privacy.[26]

> **We must work across the globe and across sectors to accelerate the sharing of cyber intelligence and best practices. We applaud WEF's efforts to change the culture and drive an increase in the skills and capabilities of the cyber defenders of aviation assets.**
>
> Jeffrey Troy, Chief Executive Officer, Aviation Information Sharing and Analysis Centre

3.2 Recommendations at national level

FIGURE 6 National level

National level

– Enabling systematic build up of skills
– Rewarding open communication on incidents

Enabling systematic build up of skills

People are an integral part of a successful cyber-defence mechanism and often the first line of defence. Aviation businesses must develop the cyber literacy of employees and provide them with the tools necessary to detect suspicious activities such as social-engineering attacks.

Going beyond typical awareness training, skill development should cover measures that guide employees in reporting suspicious activity. This would build on aviation's safety-and-security culture to develop a cybersecurity culture across all stakeholders.

Worldwide, there is a shortage of more than three million security experts.[27] National development plans should include developing a new security-centric skill set. Professionals, specifically for the aviation industry, with cybersecurity design competences for operational technology and critical infrastructure are difficult to find. To close the cybersecurity skills gap, aviation businesses should invest in the capabilities of their current employees, but also potential future employees such as students. Beyond education programmes in schools and universities, or professional training or awareness campaigns, it is necessary to include activities that foster the understanding of complex systems by modelling them in a lab or performing table-top and simulation exercises.

A national public-private approach could be advantageous. Additionally, while technical cybersecurity training is available, training services for executive leaders and boards are difficult to find. In 2018 the International Telecommunication Union issued a guide to developing a national cybersecurity strategy in conjunction with 12 public-private partners that includes a focus area on building capability and awareness.[28]

Rewarding open communication about incidents

Sharing real-time information about cyber risks should take into account national security implications, as it will need to cross national and regional boundaries. A key element in fostering information-sharing is to increase regulatory protection for victims.[29]

This would incentivize the affected parties to share information on cyberattacks and breaches without fear of repercussions, equivalent to "just culture" in safety. It would also help reduce the stigma of being the victim of, or involuntarily contributing to an attack, avoiding a blame game.

Many aviation industry stakeholders, particularly operators of critical aviation infrastructure, have an obligation to report incidents to local regulators or law-enforcement bodies. Incentivizing communicative behaviour about incidents could drive a culture shift across the global aviation industry. It would require rewarding good process implementation and problem-solving capabilities and promoting consequential learning from incidents.

For instance, the US Cybersecurity Information Sharing Act (2015) attempted to promote a culture of open communication within the US government and technology and manufacturing companies.[30] Scaled to other industries and across borders, more countries could build on this, but only if they address issues such as liability protection for threat sources.

3.3 Recommendations at organizational level

Resilience is first and foremost a leadership issue, and more a matter of strategy and culture than tactics. Most resilient organizations display similar characteristics of preparedness, adaptability, collaboration, trustworthiness and responsibility.[31]

Being resilient requires those at the highest leadership levels to acknowledge the importance of proactive risk management and focus more on the ability of the organization to absorb and recover from a cyberattack that would disrupt essential services.[32]

In 2017 key principles for cyber resilience were developed by the Forum together with a global multistakeholder community of senior business leaders.[33] They were designed to help boards and executive leadership ensure the cyber resilience of their organizations. The recommendations are divided into organizational cyber resilience (protecting your house) and ecosystem-wide cyber resilience (protecting your neighbourhood). These principles can help organizations shape a responsible course of action that balances short-term goals with medium- to longer-term imperatives.

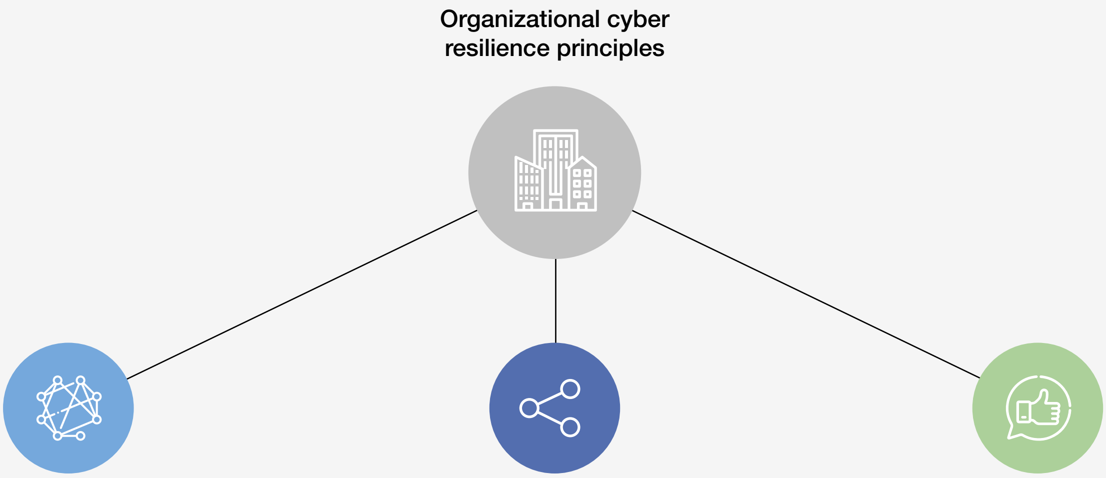
FIGURE 7 Organizational level

Organizational level

– Organizational cyber resilience principles
– Ecosystem-wide cyber resilience principles

Organizational cyber resilience principles

FIGURE 8 Organizational cyber resilience principles



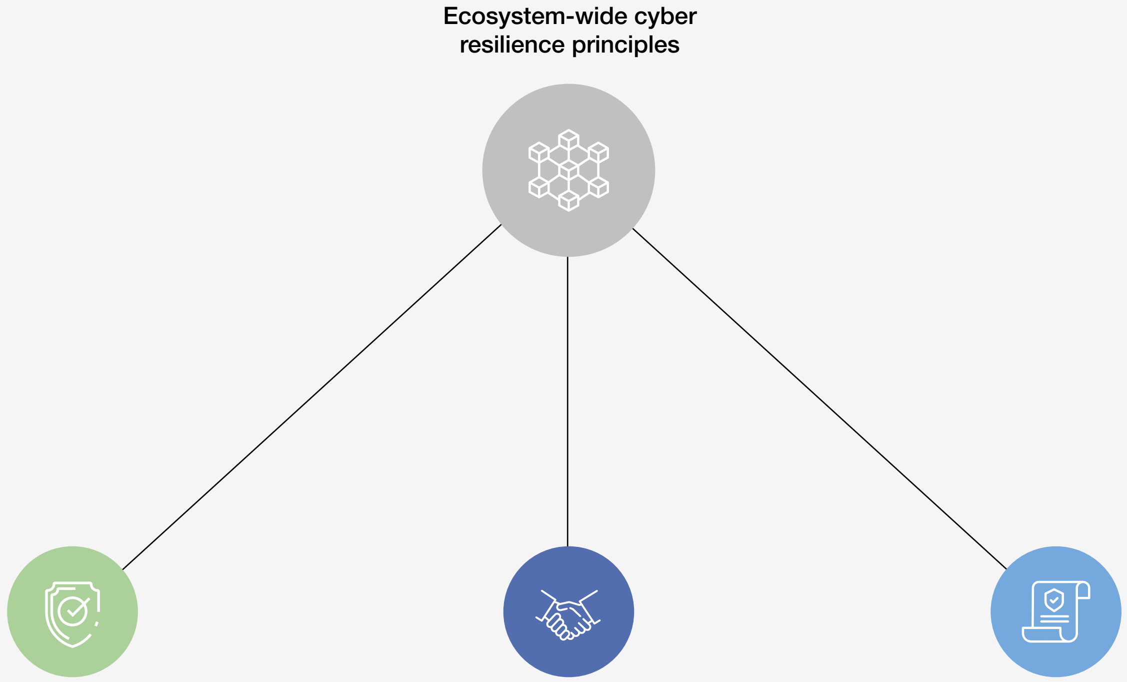
Fostering a culture of cyber resilience. The board and chief executive officer must take responsibility for oversight and drive a cultural shift. This new paradigm would entail building systems and services with the "ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems".[34] From board level down, a cyber resilience culture should be instilled in the organization, with management required to implement it and document progress.

Integrating cyber resilience into business resilience practices. Building on the robust crisis management and business continuity plans of the aviation sector, cyber resilience response and recovery practices should be integrated into the broader resilience practices of the organization.

Going beyond compliance. For aviation organizations, being compliant with regulations does not necessarily mean being secure. Moreover, with the rapid pace of digitalization, regulations may not keep up with the emerging cyber risks. As a result, aviation-sector organizations need to adopt a "risk-based approach mindset". These organizations would need to ensure their cyber risk posture and efforts extend beyond compliance, towards a holistic risk management approach.

Ecosystem-wide cyber resilience principles

FIGURE 9 Ecosystem-wide cyber resilience principles



Ensuring systemic risk assessment and prioritization. Knowing what needs to be protected is the first step to advancing systemic cyber resilience. In this industry, where every connected device represents a potential entry point for an adversarial actor, both the organization's asset base and interdependence within the ecosystem would need to be assessed. The board and chief executive officer should hold employees accountable for understanding the organization's interdependencies within the ecosystem, reporting on the systemic cyber risks posed by actors in the supply and value chains, and planning and prioritizing cyber resilience efforts accordingly.[35]

Collaborating ecosystem-wide. The board and chief executive officer need to promote collaboration and actively participate in initiatives to ensure actions are taken to secure the broader ecosystem against current and emerging cyberthreats. Furthermore, businesses must align expectations with suppliers on their cybersecurity controls (and associated compliance regimes) to encourage regulatory alignment in terms of third-party assurance, and also take forward a range of community initiatives to raise awareness of cybersecurity risks within the broader supply chain.[36]

Establishing ecosystem-wide cyber resilience plans. The board and chief executive officer should encourage employees to create, implement, test, and continuously improve collective cyber resilience plans and controls together with other members of the ecosystem. These plans should appropriately balance preparedness and protection (e.g. defence in depth strategies) with response and recovery capabilities. The COVID-19 pandemic has reminded business leaders of the importance to adapt and test their response and resilience plans regularly against different disaster scenarios with their key suppliers and business partners. This includes using these tests to challenge assumptions (such as recovery times) and to develop means to measure resilience, response, recovery and other key capabilities needed to anticipate, withstand, and recover from attacks or compromises on systems.[37]

> **The profound and dire consequences of cyberattacks are all too familiar. This report sets out a timely, pragmatic and effective framework for how aviation might better protect itself; something I hope we all can warmly embrace.**
>
> Peter Drissell, Director of Aviation Security at Civil Aviation Authority, UK

Conclusion

Aviation stakeholders recognize that building cyber resilience across the global ecosystem involves all domains of the aviation sector and requires coordinated effort. The ultimate objective is to develop a “system of systems” approach that enables civil aviation to be agile, and to adapt to a new operating model in a timely fashion, so as to withstand new attacks without significant disruptions.

In its post-COVID recovery phase, the aviation cybersecurity industry needs to augment its capacity to create a strong, safe, secure and resilient aviation sector capable of facing the new vulnerabilities that come with the next generation of technologies. Regulators and industrial-standard entities must draft and deliver cybersecurity regulations and standards, recommended practices, associated means of compliance, and guidance material. These new instruments and tools will help the industry increase its overall maturity level.

Moreover, with risks spanning multiple organizations, it is essential that stakeholders understand the end-to-end risks and the risk-management postures of the other stakeholders. Anticipating changing threats is key to helping the air transport system proactively adapt its protection strategy – not just for current threats, but also for potential future threats.

The aviation industry can build on a strong culture of safety and of handling crises and physical security events. The development and implementation of new regulations and standards tends to be slow, and alone is not sufficient to respond to the challenges ahead. Trust in a digitally connected environment must be developed between stakeholders. Multidisciplinary experts must first discuss the current threat surface, taking stock of risks to the overall ecosystem. Implementing and maintaining a common standard-of-care baseline, including robust risk-assessment methodologies, is key to establishing cyber resilience.

For the aviation industry to prosper and realize the digital dividends of the Fourth Industrial Revolution in a safe and secure manner, cyber resilience needs to be embedded in the culture and in business-operation models. The proposed pathways can be used by business and government leaders to build resilient and sustainable digital systems that are better prepared for future systemic shocks.

Appendix

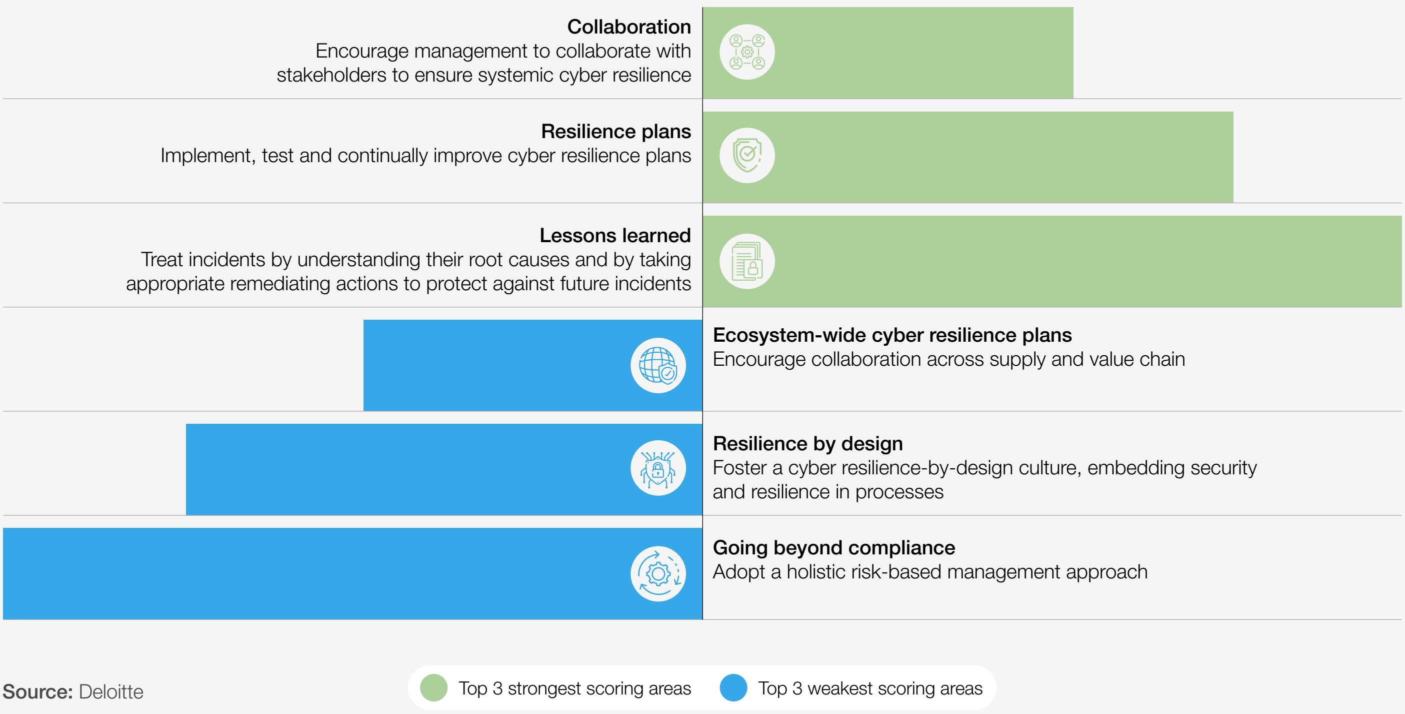
High-level results of the benchmarking exercise

From mid-September 2020 until mid-January 2021, the World Economic Forum and Deloitte carried out a benchmarking exercise with a small pilot group of aviation businesses, to assess their current cyber resilience posture.

For the purpose of this exercise, the Forum's Advancing Cyber Resilience: Principles and Tools for Boards[38], and the UK's Cyber Assessment Framework[39] were selected as frameworks. The participating organizations included air navigation service providers (ANSPs), airlines, airports, aircraft leasing companies, and holdings that represent multiple industry segments or individual players. The pilot organizations were also based in various different regions, including Asia, North America, South America and Europe.

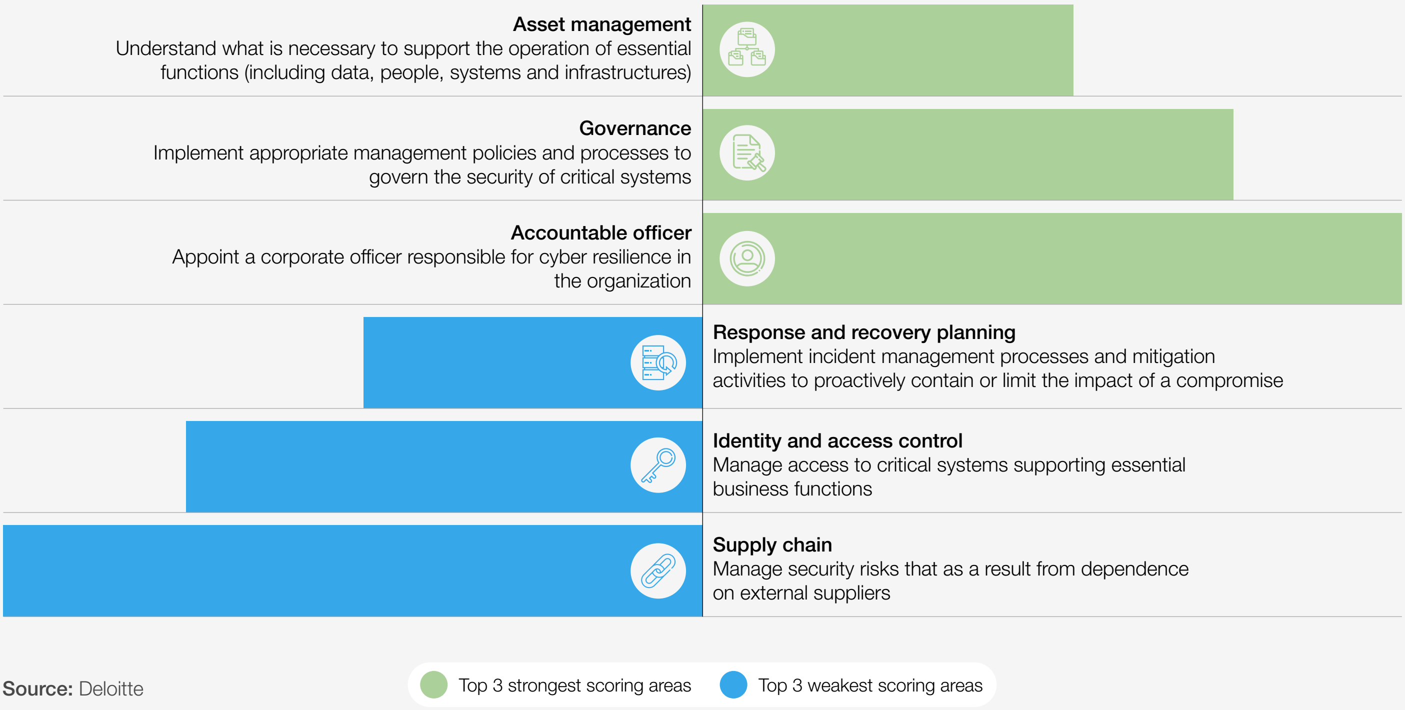
The graphs below show the high-level results of this exercise for each framework. These results are illustrative and based on a self-assessment of 14 organizations in total. As such, these results need to be interpreted with caution and do not give a generalized view on the cyber resilience posture of the aviation industry as a whole.

FIGURE 10 World Economic Forum's Advancing Cyber Resilience: Principles and Tools for Boards



Source: Deloitte

FIGURE 11 | UK Civil Aviation Authority Cyber Assessment Framework for Aviation



Source: Deloitte

Glossary

The table below provides definitions of the most-used terms throughout the document.

Term	Definition
System of systems (SoS)	A system of systems (SoS) is a collection of systems, each capable of independent operation, that interoperate together to achieve additional desired capabilities.[40]
Board and board of directors	Corporate fiduciaries responsible for overseeing management strategy, as well as the identification and planned response to enterprise-wide risks affecting a company and its value to stakeholders and shareholders.
Cyber resilience	A dimension of cyber risk management, representing the ability of systems and organizations to develop and execute long-term strategies to withstand cyber events.
Information technology (IT)	Any equipment or technique that handles information, used by a company, institution or other organization.
Operational technology (OT)	Technology that monitors and manages industrial-process assets and manufacturing/industrial equipment, in the aviation sector this would include ground and aircraft systems.

Acknowledgements

Working group

Jörg Koletzki
Group Chief Information Officer, AerCap

Sheridan Risteard
Company Secretary and Chief Compliance Officer, AerCap

Stan Barnes
Chief Financial Officer, Aergo

John Luddy
Vice President for National Security Policy, Aerospace Industries Association (AIA)

Leslie Riegle
Assistant Vice President Civil Aviation, Aerospace Industries Association (AIA)

Dennis Tracz
Senior Director Cybersecurity and Fraud, Air Canada

Serge Yonke Nquewo
Senior Manager Facilitation and IT, Airport Council International (ACI)

Marie-Caroline Laurent
Vice President Strategic Engagement, Aviation ISAC

Jeffrey Troy
President and Chief Executive Officer, Aviation ISAC

Arina Pazushko
Head External Affairs, BI.ZONE

Gareth Delany
Executive Director and Chief Technical Officer, Clover

Julie Zhu
Director and Head of General Affairs, Clover

Lucas Kelly
Information Security Manager, Corporacion America

David Thornewill von Essen
Group Chief Information Security Officer and CIO Group Functions, Deutsche Post DHL Group

Reagan Winchester
Director Information Technology, Edmonton Airport

Thomas Heuckeroth
Vice President Cybersecurity, Emirates Group

Chris Sedgwick
Director Marketing and Communications, Falko

Bithal Bhardwaj
Group Chief Information Security Officer, GMR Group

David Mabry
Chief Information Security Officer, Gulfstream Aerospace Corporation

Melissa Frydrych
Cyber Threat Hunt Analyst, IBM

Julian Meyrick
Managing Partner and Vice President, IBM

Claire Zaboeva
Senior Strategic Cyber Threat Analyst, IBM

Stephen Mellor
Chief Technology Officer, Industrial Internet Consortium

Jerry Hancock
Director Cyber Security for Aviation, Inmarsat Global

William Harvey
Head Cybersecurity Assurance and Compliance, International Airlines Group (IAG)

Jonathan Lloyd White
Chief Information Security Officer, International Airlines Group (IAG)

Pascal Buchner
Director ITS & Chief Information Officer, International Air Transport Association (IATA)

Rashad Karaky
Aviation Cybersecurity Officer, International Civil Aviation Organization (ICAO)

Matthew Vaughan
Director Aviation Security, International Air Transport Association (IATA)

Dadi Gertler
Chief Technology Officer and Business Development, Israel National Cybersecurity Directorate

Abdou-Naby Diaw
Chief Information Security Officer, Lufthansa Group

Jean-Francois Tanguay
IT Security Manager, Montreal Airport

Tom Bornais
Director of the Enterprise Technology Security Office, NavCanada

Kerry-Ann Barrett
Cybersecurity Policy Specialist, Organization of American States (OAS)

Scott Boyle
Director Information Technology and Telecommunications, Ottawa International Airport

Jean-Claude Yao
Manager IT Compliance, Ottawa International Airport

Jason Deluce
Director Information Technology, Porter

Vikram Sharma
Chief Executive Officer, Quintessence Labs

Ian Law
Chief Information Officer and Airport Deputy Director, San Francisco Airport

Zenia Laxa
Cyber Security Engineer, San Francisco Airport

Terrence Ng
Chief Information Security Officer, Singapore Airlines

Martina Costelloe
Information Security Manager, SMBC Aviation Capital

Christian Keller
Head of Information Security, Swiss International Airlines

Tippawan Pornkongcharoen
Senior IT Specialist - IT Security and Quality Assurance Management Department, Thai Airways

Laurent Kettela
Head of Cyber Security and Transformation Program, Thales Group

Peter Drissell
Director Aviation Security, UK Civil Aviation Authority

Andrew Cocking
Security Assurance Manager, UK NATS

Joe Dauncey
Chief Information Security Officer and Chief Security Officer, UK NATS

Deneen DeFiore McGarvey
Chief Information Security Officer, United Airlines

Gan Subramaniam
Head of Information Security, UPS

Bernie Ip
Director Technology Services, Vancouver Airport

Jennifer Farquhar
Director Global Communications and Brand Marketing, Vistajet

Dan Neal
Chief Information Security Officer, Westjet Airlines

Lori Bailey
Global Head of Cyber Risk, Zurich Insurance Group

Contributors

World Economic Forum

Georges de Moura
Head of Industry Solutions, Centre for Cybersecurity

Jeff Merritt
Head of Internet of Things and Urban Transformation

Lauren Uppink
Head of Aviation, Travel and Tourism Industries

Geoff Wylde
Lead, Internet of Things and Urban Transformation

The World Economic Forum extends its gratitude to the contributors who helped to produce this Insight Report.

Deloitte

Laura Coman
Senior Manager, Deloitte, Belgium

Camille De Landtsheer
Senior Consultant, Deloitte, Belgium

Ines Fichtinger
Senior Consultant, Deloitte, Belgium

Chris Verdonck
Partner, Deloitte, Belgium

Advisory committee

Nina Brooks
VP Facilitation, Security and Innovation, Airport Council International (ACI)

Kesang Ukyab
Manager Innovation and Technology, Airport Council International (ACI)

Jean-Paul Moreaux
Principal Cybersecurity in Aviation Coordinator, European Aviation Safety Agency (EASA)

Patrick Mana
Cybersecurity EATM-CERT Manager, EUROCONTROL

Manon Gaudet
Assistant Director Aviation Cybersecurity, International Air Transport Association (IATA)

Saulo Da Silva
Chief Global Interoperable Systems Section, International Civil Aviation Organization (ICAO)

Sylvain Lefoyer
Deputy Director of Aviation Security and Facilitation, International Civil Aviation Organization (ICAO)

Dan Carnelly
Senior Director Technology, International Coordinating Council of Aerospace Industries Associations (ICCAIA)

Nicky Keeley
Head of Cybersecurity Oversight, UK Civil Aviation Authority

Dr. Kevin Thacker
Head of Support to Cyber Regulation, UK National Cyber Security Centre

Endnotes

1. “Airport cybersecurity in a COVID-19 world”, accessed 28 March 2021, https://blog.aci.aero/airport-cybersecurity-in-a-covid-19-world/
2. The Global Risk Report 2021, accessed 28 March 2021, http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf
3. “Developing Cyber Resilient Systems: A Systems Security Engineering Approach”, accessed 28 March 2021, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf
4. “Cybersecurity Leadership Principles: Lessons learnt during the COVID-19 pandemic to prepare for the new normal”, May 2020, accessed 28 March 2021, http://www3.weforum.org/docs/WEF_Cybersecurity_leadership_principles_for_the_Covid_19_pandemic_2020.pdf
5. “Airport Cybersecurity COVID-19 Survey Report 2020”, accessed 28 March 2021, https://store.aci.aero/product/airport-cybersecurity-covid-19-survey-report-2020/
6. “ENISA Threat Landscape 2020 – Ransomware”, accessed 28 March 2021, https://www.enisa.europa.eu/publications/ransomware
7. “Airlines warn passengers of data breach after aviation tech supplier is hit by cyberattack”, accessed 28 March 2021, https://www.zdnet.com/article/airlines-warn-passengers-of-data-breach-after-aviation-tech-supplier-is-hit-by-cyberattack/
8. “ICAO Aviation Cybersecurity Strategy”, October 2019, accessed 28 March 2021, https://www.icao.int/cybersecurity/Documents/AVIATION%20CYBERSECURITY%20STRATEGY.EN.pdf
9. ICAO, “THIRTEEN AIR NAVIGATION CONFERENCE”, accessed 28 March 2021, https://www.icao.int/Meetings/anconf13/Documents/WP/wp_160_en.pdf
10. ICAO, “THIRTEEN AIR NAVIGATION CONFERENCE”, accessed 28 March 2021, https://www.icao.int/Meetings/anconf13/Documents/WP/wp_160_en.pdf
11. “Aviation cybersecurity: Scoping the challenge”, accessed 28 March 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/aviation-cybersecurity-scoping-the-challenge-report/
12. “Future Series: Cybersecurity, emerging technology and systemic risk”, November 2020, accessed 28 March 2021, http://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf
13. “5G Market in Aviation by End Use”, accessed 28 March 2021, https://www.marketsandmarkets.com/Market-Reports/5g-market-aviation-152979610.html
14. “Cyber Resilience in the Electricity Ecosystem: Securing the Value Chain”, December 2020, accessed 28 March 2021, http://www3.weforum.org/docs/WEF_Securing_the_Electricity_Value_Chain_2020.pdf
15. “Aviation cybersecurity: Scoping the challenge”, accessed 28 March 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/aviation-cybersecurity-scoping-the-challenge-report/
16. ICAO, “ASSEMBLY – 39TH SESSION”, accessed 28 March 2021, https://www.icao.int/Meetings/a39/Documents/WP/wp_493_en.pdf
17. “NCSC CAF Guidance: Introduction to the Cyber Assessment Framework”, National Cyber Security Centre https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework; see also “The Information Commissioner’s response to the Ofgem consultation Standards of Conduct for suppliers in the retail energy market”, Information Commissioner’s Office, 13 March 2017, accessed 16 June 2020, https://www.ofgem.gov.uk/ofgem-publications/117734
18. “Advancing Cyber Resilience in Aviation: An Industry Analysis”, accessed 28 March 2021, https://www.weforum.org/whitepapers/advancing-cyber-resilience-in-aviation-an-industry-analysis
19. “Advancing Cyber Resilience: Principles and Tools for Boards”, accessed 28 March 2021, https://www.weforum.org/whitepapers/advancing-cyber-resilience-principles-and-tools-for-boards
20. “Cyber security compliance”, UK CAA, accessed 28 March 2021, https://www.caa.co.uk/Commercial-industry/Cyber-security-oversight/Cyber-security-compliance/
21. “NCSC CAF Guidance: Introduction to the Cyber Assessment Framework”, National Cyber Security Centre, https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework; see also “The Information Commissioner’s response to the Ofgem consultation Standards of Conduct for suppliers in the retail energy market”, Information Commissioner’s Office, 13 March 2017, accessed 16 June 2020, https://www.ofgem.gov.uk/ofgem-publications/117734
22. “Cyber Strategy Framework”, accessed 28 March 2021, https://www2.deloitte.com/be/en/pages/risk/solutions/cyber-strategy-framework.html
23. “Cybersecurity Leadership Principles Lessons learnt during the COVID-19 pandemic to prepare for the new normal”, accessed 28 March 2021, http://www3.weforum.org/docs/WEF_Cybersecurity_leadership_principles_for_the_Covid_19_pandemic_2020.pdf

24. “Cybersecurity Leadership Principles Lessons learnt during the COVID-19 pandemic to prepare for the new normal”, accessed 28 March 2021, http://www3.weforum.org/docs/WEF_Cybersecurity_leadership_principles_for_the_Covid_19_pandemic_2020.pdf

25. “Future Series: Cybersecurity, emerging technology and systemic risk”, November 2020, accessed 28 March 2021, http://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf

26. “Future Series: Cybersecurity, emerging technology and systemic risk”, November 2020, accessed 28 March 2021, http://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf

27. “Cybersecurity Professionals Stand Up to a Pandemic”, accessed 28 March 2021, https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B

28. “Guide to developing a national cybersecurity strategy”, ITU, accessed 28 March 2021, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

29. “Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards”, accessed 28 March 2021, http://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf

30. “Cybersecurity Information Sharing Act of 2015”, accessed 28 March 2021, https://www.cisecurity.org/newsletter/cybersecurity-information-sharing-act-of-2015/

31. “Building The Resilient Organization”, accessed 28 March 2021, https://www2.deloitte.com/content/dam/insights/articles/US114083_Global-resilience-and-disruption/2021-Resilience-Report.pdf?ic

32. “Cybersecurity Leadership Principles Lessons learnt during the COVID-19 pandemic to prepare for the new normal”, accessed 28 March 2021, http://www3.weforum.org/docs/WEF_Cybersecurity_leadership_principles_for_the_Covid_19_pandemic_2020.pdf

33. “Advancing Cyber Resilience: Principles and Tools for Boards”, accessed 28 March 2021, https://www.weforum.org/whitepapers/advancing-cyber-resilience-principles-and-tools-for-boards

34. “NIST Special Publication 800-160 Volume 2”, accessed 28 March 2021, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf

35. “Advancing Cyber Resilience: Principles and Tools for Boards”, accessed 28 March 2021, https://www.weforum.org/whitepapers/advancing-cyber-resilience-principles-and-tools-for-boards

36. “Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards”, accessed 28 March 2021, http://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf

37. “Cybersecurity Leadership Principles Lessons learnt during the COVID-19 pandemic to prepare for the new normal”, accessed 28 March 2021, http://www3.weforum.org/docs/WEF_Cybersecurity_leadership_principles_for_the_Covid_19_pandemic_2020.pdf

38. Advancing Cyber Resilience: Principles and Tools for Boards, accessed 28 March 2021, https://www.weforum.org/whitepapers/advancing-cyber-resilience-principles-and-tools-for-boards

39. UK CAA Cyber security compliance, accessed 28 March 2021, https://www.caa.co.uk/Commercial-industry/Cyber-security-oversight/Cyber-security-compliance/

40. “Systems of Systems”, Mitre, accessed 28 March 2021, https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-of-systems

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