Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

# AVIATION CYBERSECURITY

## Scoping the Challenge

Pete Cooper
with Simon Handler and Safa Shahwan

Underwritten by
THALES

**The Scowcroft Center for Strategy and Security** works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

**The Cyber Statecraft Initiative** works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

# AVIATION CYBERSECURITY

## Scoping the Challenge

Pete Cooper
with Simon Handler and Safa Shahwan

ISBN-13: 978-1-61977-080 5

Cover: Singapore Changi Airport



Atlantic Council
1030 15th Street, NW
12th Floor
Washington, DC 20005

Website: www.atlanticcouncil.org

# Foreword

In the past decade, the aviation industry has reaped the benefits of digitization. With the aircraft efficiency gains and enhancements to the passenger experience catalyzed by new technologies, we have to acknowledge the corresponding new risks, including social and technical vulnerabilities never before addressed. In 2017, the Atlantic Council released its groundbreaking report, *Aviation Cybersecurity—Finding Lift, Minimizing Drag*. The report raised awareness on the state of cybersecurity in the aviation industry, sparking public dialogue on the intersection of cybersecurity and aviation. This created a foundation for the aviation community to convene around protecting the traveling public. Since then, it has become evident that anticipating, identifying, and mitigating cyberspace vulnerabilities in aviation will require the buy-in of all stakeholders in this ecosystem.

Two years on, Thales is honored to continue its support for the Atlantic Council and this crucial initiative that aims to map perspectives on cybersecurity across this diverse industry and highlight the growing need for collaboration across stakeholders. Ultimately, there is no silver bullet for aviation cybersecurity, and confronting cyber risk in aviation will require a global approach, working across safety, security, cybersecurity, and enterprise IT. This report and the accompanying global survey developed by the Atlantic Council will increase our holistic understanding of aviation cyber risk and drive meaningful engagement across the aviation community.

This effort to broaden the community of stakeholders examining cybersecurity in aviation will increase our collective security, safety, and resilience. When it comes to the trust of travelers, we are all only as strong as those most vulnerable among us. It is only through mutual understanding and collaboration that we can continue to challenge one another, grow, and improve. I applaud the Atlantic Council for embracing this topic and am proud Thales has the chance to support this work.

Sincerely,

**Alan Pellegrini**

*CEO, Thales North America*
*Board Director, Atlantic Council*

# Executive Summary

The objective of this report is to capture and understand the diversity of perspectives on aviation cybersecurity. The range of opinions and perspectives became apparent in the 2017 report, *Aviation Cybersecurity—Finding Lift, Minimizing Drag*. In that report, perspectives ranged from a belief that there was no aviation-cybersecurity challenge, because "it wasn't possible to hack" aviation systems, to the belief that there is significant, systemic risk in aviation.

The 2017 report called out the complexity of the global aviation-cybersecurity challenge and focused on the leadership role of the International Civil Aviation Organization (ICAO) as critical to drive coordinated, strategic change. ICAO took a positive step toward asserting its leadership in October 2019, when the 40th Session of the ICAO General Assembly adopted Assembly Resolution A40-10 Addressing Cybersecurity in Civil Aviation and urged states to implement the Aviation Cybersecurity Strategy, laying out both a vision and strategic goals. The significance of this development for bringing coherence to global aviation cybersecurity cannot be underestimated.

This report builds on the challenges raised two years ago to explore how these diverse perspectives have changed in the intervening time. The digital attack surface the aviation sector presents to its adversaries continues to grow in such a way that both managing risk and gaining insight on it remain difficult. With emerging technologies like machine learning and fifth-generation (5G) telecommunications seeing wider adoption—alongside electric vertical takeoff and landing (eVTOL), autonomous aircraft, and increased use of space—aviation-cybersecurity risk management is on the cusp of becoming more complex.

This report leverages a global survey of 244 respondents (in whole or in part) together with targeted interviews and several expert workshops to explore the diverse challenges of aviation cybersecurity. Although there are multiple initiatives on the topic, management of aviation-cybersecurity risk remains challenging. The first set of challenges involved issues in trying to weave aviation cybersecurity into flight safety, security, and enterprise information technology (IT), all of which have well-established governance and accountability frameworks. The second set of challenges orbits the relationship between aviation-sector suppliers and customers regarding cybersecurity, with many finding it difficult to incorporate best practices into purchases, as well as difficulties in developing consensus on adequate cybersecurity risk management and transparency.

Managing aviation cybersecurity requires making thoughtful choices from a clear and well-informed understanding of risk. Here, despite ample challenges, there are some glimmers of hope. But, on topics such as information sharing, it was clear that respondents thought there was much more to be done. Additionally, there is a clear desire for increased objectivity regarding aviation-cybersecurity risk, whether through independent assessment or agreement among aviation-sector stakeholders. There was strong agreement that good-faith researchers were a positive thing for the aviation industry, but perspectives on guidance, legal clarity, and ease of vulnerability disclosure all remain unclear or difficult to navigate.

Through both its designs and its training practices, the aviation sector rigorously works to anticipate, mitigate, and objectively investigate failure, but incorporating cybersecurity into this culture remains a challenge. There is very little operational training (for pilots, air-traffic controllers, etc.) to either recognize or manage aviation-cybersecurity incidents. And, although aviation operations are inherently resilient, disruptive attacks at scale will prove challenging to manage. Additionally, attacks against data integrity, "second-generation" attacks, undermine the ability of aviation operators to conduct safe operations. Working through these issues will require an increased effort to understand cybersecurity aspects of everything from normal operations and procedures to post-accident and incident management.

There has been increased focus on, and increased efforts toward, aviation-cybersecurity regulations and standards, but the survey conducted for this report found deep concern about their effectiveness, clarity, and communication. What was clear is that a majority of contributors thought that aviation cybersecurity should be led globally. As national, regional, and organizational efforts are under way to improve aviation cybersecurity, there is a growing risk of adding complexity across the landscape of regulations and best practices. All regions deserve the tools to improve, and any new body of standards must be harmonized across complex global supply and operations chains.

Improving aviation cybersecurity is a journey, and every stakeholder must be able to make the trip if global, systemic risk is to be reduced. ICAO promotes this from a capacity-building perspective with a tagline of "No Country Left Behind." As global aviation-cybersecurity efforts ramp up, adopting a tagline of "No Vulnerability Left Behind" is a fitting example of how focus must be applied if the sector is to remain safe, secure, and resilient.

# 1: Top-Line Actions

## This report recommends the following next steps for the aviation ecosystem

### 1.1 Global standards for a global industry

With publication of the ICAO Cybersecurity Strategy, there is now a vision for how aviation cybersecurity can advance globally.

"ICAO's vision for global cybersecurity is that the civil aviation sector is resilient to cyber-attacks and remains safe and trusted globally, whilst continuing to innovate and grow."

To coherently gain insight, understand and manage aviation-cybersecurity risk, and bring swift, globally aligned, and effective change, all aviation stakeholders—including states, international bodies, regulators, manufacturers, and service providers—are strongly encouraged to act in unison, and to support the new ICAO Cybersecurity Strategy, as called for in the ICAO Assembly Resolutions A40-10 *Addressing Cybersecurity in Civil Aviation*.[1]

### 1.2 Increasing transparency and trust

Trust in aviation cybersecurity will only come with increased transparency. Limited or ineffectual information sharing is leading to opacity of risk among stakeholders, and arguably obfuscates the scale of the aviation-cybersecurity challenge and the way forward. Actions to improve this fall into two key areas: contracts and system design.

#### 1.2.1 Contracts

All contracts between aviation stakeholders must include cybersecurity considerations, such as through-life risk management, vulnerability management, and data sharing. These must be clearly and transparently agreed upon, to ensure that all stakeholders are able to make informed decisions about cybersecurity risk.

#### 1.2.2 System design

Aviation-system design must be approached from the perspective of not only securing systems, but also increasing cybersecurity risk transparency and objectivity, for manufacturer and customer alike. All stakeholders must, therefore, be able to access and analyze their cybersecurity-relevant data. Additionally, efforts must be taken to reduce the rapidly expanding digital attack surface of the aviation sector, with a default of designing for simplicity, security, and resiliency.

### 1.3 Building bridges

The scale and complexity of the cybersecurity challenges facing the industry mean diverse stakeholders must be encouraged to support and learn from each other. There are three key areas.

#### 1.3.1 Diverse stakeholders

Because of the scale, nature, and variety of the aviation sector, a number of diverse stakeholder groups can productively collaborate to help understand and manage risk. Ranging from other sectors to cybersecurity researchers, creating a rich and positive dialogue will accelerate the understanding of the challenge, as well as potential solutions.

#### 1.3.2 Regulations and standards

ICAO, states, and standards bodies must be supported in the creation of informed and balanced aviation-cybersecurity regulations, through input from diverse stakeholders, as a collaborative and structured effort to promote global coherency.

#### 1.3.3 Safety, security, enterprise cybersecurity, and aviation cybersecurity

Where aviation cybersecurity crosses the traditional elements of aviation security, safety, and enterprise IT, efforts must be made to break down silos and create a shared vision of risk.

### 1.4 Information sharing

Cybersecurity information sharing must be approached in the same way as information sharing on the topic of flight safety. Moving to a "learn once, share widely" model will promote rapid visibility, mitigation, and management of risk across the entire sector. Blockers of information sharing on aviation cybersecurity must be critically assessed, and standards must promote the sharing of cybersecurity-relevant information in a timely and responsive manner that gets defenders ahead of vulnerabilities and adversaries.

1 "Aviation Cybersecurity Strategy," International Civil Aviation Organization, October 2019, https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx.


Airplanes at Seattle–Tacoma International Airport.

### 1.5 Communications

Aviation cybersecurity is a critical and complex topic that is still little discussed outside the sector, leading to risks of misperception and inaccuracy. Increasing external dialogue on the topic and helping create informed positions will go a considerable way toward increasing understanding and trust across multiple stakeholders.

### 1.6 People

The global scale of the aviation-cybersecurity challenge means that it now touches every single element of the sector. Already, the sector does not have enough cybersecurity staff, and this shortage will only become more acute as initiatives and efforts increase. Global, sector-wide, coordinated efforts must be made to increase the cybersecurity skills of those already in the sector, as well as to create pathways and incentives for those wanting to embark on an aviation-cybersecurity career.

### 1.7 Passenger privacy and cybersecurity

How the aviation sector protects passenger privacy and cybersecurity must be a proactive and transparent dialogue. Starting discussions now on the topic of passenger privacy and security will also make it easier to develop appropriate supporting frameworks, reduce noncompliance risks, and scale technology such as biometrics.

# Table of Contents

# List of Abbreviations

**IATA** — International Air Transport Association

**ATM** — Air-Traffic Management

**ALARP** — As Low As Reasonably Practicable

**IT** — Information Technology

**ICAO** — International Civil Aviation Organization

**IP** — Intellectual Property

**FAA** — Federal Aviation Association

**ASISP** — Aircraft Systems Information Security Protection

**ADD** — Aircraft-Data Domains

**SOC** — Security-Operations Center

**EASA** — European Aviation Safety Agency

**OEM** — Original Equipment Manufacturers

**UAM** — Urban Air Mobility

**PNT** — Positioning, Navigation, and Timing

**CVP** — Coordinated Vulnerability Programs (CVP)

# 2: Introduction and Overview

## 2.1 THE AIM OF THE SURVEY AND REPORT

Like many other sectors, aviation is digitized, connected, and potentially vulnerable to malicious cyber adversaries and activities. Because it is a global, interconnected, and interdependent sector, any disruption can quickly ripple out to have international impacts, cause significant financial and reputational damage, and potentially compromise safety. The digital attack surface of the aviation sector has never been larger than it is today, as more and more digitized and connected services are developed for sound reasons such as efficiency and passenger service. Understanding how to manage and protect this burgeoning attack surface, while building in resiliency, is arguably the most pressing security challenge facing the aviation sector.

This report uses the results of a survey, workshops, and interviews with those involved in aviation cybersecurity, and explores the risks, challenges, opportunities, and suggested actions for a resilient and cyber-secure global aviation sector.

To do this, voices were explored from across the sector: aircraft and airport operations, manufacturers, air-traffic control, maintenance, repair and overhaul, security, the supply chain, regulators, government, and those that support from outside the sector, such as the cybersecurity research community. All of these stakeholders have valuable perspectives, but nobody has ever been able to engage so deeply on the topic, capture their voices, understand their perspectives, and learn from them, until now.

The 2017 report, *Finding Lift, Minimizing Drag*, highlighted that the diversity of perspectives on the nature and severity of the cybersecurity challenge facing the aviation sector was potentially holding back tangible progress.[2] Some stakeholders proffered that there was very little cybersecurity risk in aviation, while others said that it was a critical, complex, and little understood challenge, and that only once a cyberattack took place would there be tangible progress. With the increased focus on global aviation cybersecurity, ranging from the new ICAO Cybersecurity Strategy to new security standards both in Europe and the United States, alongside increasing adversary efforts to target the aviation sector, the coming years will be challenging ones.

The topics discussed within this report and its findings are valuable not just for the aviation sector, but all complex, digitized, connected industries. It is not a lack of available technology that affects how people address the cyber challenge, but rather the level and maturity with which they perceive these challenges. The complexity and rapid pace of digital evolution are now the norm, and can no longer be used as a reason for the difficulty of defending that which is critical. Collectively moving forward, gaining focus, and developing clear intent to manage aviation-cybersecurity risks will require partnerships across diverse perspectives and stakeholders; this will allow the sector to quickly and collaboratively improve.

2 Pete Cooper, *Aviation Cybersecurity—Finding Lift, Minimizing Drag*, Atlantic Council, November 7, 2017, https://www.atlanticcouncil.org/in-depth-research-reports/report/aviation-cybersecurity-finding-lift-minimizing-drag/.

# 3: Scope

Aviation cybersecurity is a topic that straddles many silos; therefore, defining its scope is essential. For the purposes of this report, aviation cybersecurity is defined as cybersecurity pertaining to aviation operations.

This may seem a simple melding of cybersecurity and aviation, but simplicity must be the key. Across the sector, the focus is very much on maintaining safe and secure aviation operations. This encompasses airliners, future urban air mobility (UAM) vehicles, commercial space travel (which must transit through "legacy" airspace), and everything that supports aviation operations, ranging from ground assets to space-based communications and positioning, navigation, and timing (PNT). To allow for this breadth and for future developments, cybersecurity in aviation must also align with this scope.

## METHODOLOGY

The purpose of this report is to gain insight on aviation-cybersecurity perspectives across a wide demographic. With such a challenging topic, this was approached in a number of ways. First, focus areas were developed from the 2017 report, Finding Lift, Minimizing Drag, as well as interviews with those involved in aviation cybersecurity and observations from across the sector. From these topic areas, questions were developed that allowed for the creation of a survey that was distributed across the sector. The 244 respondents to participate in the survey (in whole or in part) spanned the breadth of the aviation industry, with occupational backgrounds including: aircraft operations; airports; air-traffic management; aviation services; maintenance, repair, and overhaul; original equipment manufacturing; and cybersecurity research. Responses from the survey were then triangulated in a series of workshops and interviews that explored and amplified the gathered perspectives.

# 4: Vision

The 40th Session of the ICAO General Assembly adopted its first Cybersecurity Strategy relating to aviation in October 2019, stating the following vision.

*"ICAO's vision for global cybersecurity is that the civil aviation sector is resilient to cyber-attacks and remains safe and trusted globally, whilst continuing to innovate and grow."*[3]

This vision, the first for ICAO, highlights the key challenges facing the sector. The importance of resilience sits alongside the need for safety and maintaining trust at the same time, while still embracing growth and innovation. This report strongly supports such a vision, as it brings global coherence to both the challenge and direction of travel.

3 "Aviation Cybersecurity Strategy," International Civil Aviation Organization.

# 5: The Aviation-Cybersecurity Landscape

It is fair to say that the aviation sector has now fully embraced digitized, connected technologies; this is most evident in the evolution of eEnabled aircraft. The nature of that evolution is laid out by the US Federal Aviation Administration (FAA).

*"New aircraft designs use advanced technology for the main aircraft backbone connecting flight-critical avionics as well as passenger information and entertainment systems in a manner that makes the aircraft an airborne interconnected network."*[4]

It describes the internal aircraft network as follows.

*"The architecture of this airborne network may allow read and/or write access to and/or from external systems and networks, such as wireless airline operations and maintenance systems, satellite communications, email, the internet, etc. Onboard wired and wireless devices may also have access to portions of the aircraft's digital data buses (DDB) that provide flight critical functions."*

It also goes on to highlight some of the myriad risks.

*"Connected aircraft have the capability to reprogram flight critical avionics components wirelessly and via various data transfer mechanisms. This capability alone, or coupled with passenger connectivity on the aircraft network, may result in cybersecurity vulnerabilities from intentional or unintentional corruption of data and/or systems critical to the safety and continued airworthiness of the airplane."*

As much as the FAA has laid out formal wording, an eEnabled aircraft can be more simply summarized as a flying data center that continually travels around the globe, with connected safety-critical systems, multiple connections over wired and wireless bearers, and multiple service suppliers both while on the ground and while airborne. It's easy to see why the cybersecurity of such a platform is as critical as it is challenging.

Increased digitization of air-traffic management (ATM) and information systems is also continuing at pace, as the sector seeks to increase airspace capacity and throughput. At the cutting edge of this is the ICAO Trust Framework project, which aims to securely and digitally connect aviation assets and units around the globe to facilitate information sharing that will be used for multiple purposes, including real-time traffic management.[5] Alongside increasing traffic density and variety from platforms such as UAM and unmanned aerial vehicles (UAV), digitization is enabling greater situational awareness and reduced separations based on trajectory, not just height or location.

Airports are also increasingly connected and digitized, with many of these services also having remote or wireless connections. These range from access-control and airside systems such as maintenance, tugs, and high-speed wireless links between the aircraft and docking gate.[6] All of these digitized services exist against a backdrop of complex airport management and accountability, making it difficult to holistically define and defend such an attack surface.

Many of these services—spanning aircraft, ATM, and airport—increasingly rely on space-based assets for their operations, ranging from data transfer and communications to PNT. As legacy and analog capabilities are phased out in favor of space-based

4 "Flight Standards Information Management System (FSIMS)," US Department of Transportation, Federal Aviation Agency, 2007, 633, https://www.faa.gov/documentLibrary/media/Order/8900.1.pdf.

5 "A40 SkyTalks: Aviation Benefits," Uniting Aviation, October 24, 2019, https://www.unitingaviation.com/video/skytalks/a40-skytalks-aviation-benefits/.

6 Ken Munro, "Mapping the Attack Surface of an Airport," Pen Test Partners, October 11, 2019, https://www.pentestpartners.com/security-blog/mapping-the-attack-surface-of-an-airport/.

capabilities, their cybersecurity and resiliency must increasingly be scrutinized. One contributor described the cybersecurity posture of some space assets as stuck in the 1980s.

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.[7] 5G will likely become a ubiquitous means of communications across every aspect of the aviation sector, with advantages based on size (connectivity at "chip level"), low-power requirements, and flexibility.[8] But, 5G has several cybersecurity challenges, with the European NIS Cooperation group asserting, "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.[9]

Overall, the challenge of understanding risk across interdependent and complex digitized aviation systems, with an extensive supply chain, is only increasing. Other sectors have seen the scale and costs from a single vulnerability and "wormable" exploit. Given the criticality of the sector, combined with disruptions that could scale rapidly, there remains much to do to understand the aviation-cybersecurity landscape.

## 5.1 AVIATION-CYBERSECURITY PROGRESS

Against this background of challenges, there has been increasing dialogue and action on aviation cybersecurity across the entire sector. In 2017, *Finding Lift, Minimizing Drag* proposed that, at a global level, it would "take leadership from the top down to improve governance and accountability in the global aviation ecosystem."[10] The publication of the first Aviation Cybersecurity Strategy by ICAO in October 2019 was a critical first stage in building global coherency, and has gone a significant way to signpost direction.

Additionally, the publication of the European Strategic Coordination Platform Strategy for Cybersecurity in Aviation is a significant step forward at a regional level, and sits alongside national efforts such as the UK Aviation Cybersecurity Strategy.[11]

From an aviation-cybersecurity-standards perspective, there has been significant activity by both the European Aviation Safety Agency (EASA) and the US FAA. By the close of 2019, the only way that aircraft, aviation systems, engines, etc. will be able to achieve airworthiness certification is to comply with the recently updated DO-326 and ED-202.[12] These new regulations are considerably more detailed and comprehensive in their approach to the management of cybersecurity risk.

Additionally, a new initiative of the US Department of Homeland Security (DHS), in partnership with the US Air Force (USAF), will increase scrutiny of aircraft cybersecurity.[13] Following the publication of the US National Strategy for Aviation Security and the creation of the Aviation Cybersecurity Initiative (ACI), chaired jointly by DHS's Cybersecurity and Infrastructure Security Agency, US Department of Defense (DoD), and the US Department of Transportation (DoT), the new initiative includes conducting vulnerability assessments of aircraft as a means to better understand and mitigate risk.[14]

Gaining insight to risk is a fundamental requirement for the aviation sector. For example, if a potential flight-safety issue were raised, the safety management system (SMS) would be systematic and proactive in terms of managing that risk; arguably, the management of cybersecurity risk in aviation should be no different.[15] Therefore, it is heartening to see organizations such as Boeing now providing guidance on how security researchers can submit potential cybersecurity vulnerabilities.[16] Other regional bodies—such as the European Centre for Cybersecurity in Aviation (ECCSA, part of EASA), as well as the

7 "5G Market in Aviation by End Use (5G Infrastructure for Aircraft and Airport), Technology (EMBB, FWA, URLLC/MMTC), Communication Infrastructure (Small Cell, DAS), 5G Services (Aircraft Operations, Airport Operations), Region—Global Forecast to 2026," Markets and Markets, August 2019, https://www.marketsandmarkets.com/Market-Reports/5g-market-aviation-152979610.html.

8 Douglas Busvine, "Huawei Shows off All-in-One 5G System on a Chip," *Disruptive.Asia*, September 9, 2019, https://disruptive.asia/huawei-5g-system-on-a-chip/.

9 "EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks," NIS Cooperation Group, October 2019, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132.

10 Cooper, *Aviation Cybersecurity—Finding Lift, Minimizing Drag*.

11 "Strategy for Cybersecurity in Aviation," European Strategic Coordination Platform, September 2019, https://www.easa.europa.eu/sites/default/files/dfu/Cybersecurity%20Strategy%20-%20First%20Issue%20-%2010%20September%202019.pdf; "Aviation Cybersecurity Strategy," UK Department for Transport, Civil Aviation Authority, July 12, 2018, https://www.gov.uk/government/publications/aviation-cyber-security-strategy.

12 Aharon David, "How DO-326 and ED-202 Are Becoming Mandatory for Airworthiness," *Aviation Today*, May 1, 2019, https://www.aviationtoday.com/2019/05/01/326-ed-202-becoming-mandatory-airworthiness/.

13 Robert McMillan and Dustin Volz, "U.S. Steps Up Scrutiny of Airplane Cybersecurity," *Wall Street Journal*, September 29, 2019, https://www.wsj.com/articles/u-s-government-steps-up-scrutiny-of-airplane-cybersecurity-11569764123.

14 "National Strategy for Aviation Security of the United States of America," White House, December 2018, https://www.whitehouse.gov/wp-content/uploads/2019/02/NSAS-Signed.pdf; McMillan and Volz, "U.S. Steps Up Scrutiny of Airplane Cybersecurity."

15 "Safety Management Systems," UK Department for Transport, Civil Aviation Authority, last visited November 19, 2019, https://www.caa.co.uk/Safety-initiatives-and-resources/Working-with-industry/Safety-management-systems/Safety-management-systems/.

16 "Ethics and Compliance," Boeing, last visited November 19, 2019,

ICAO Cybersecurity Strategy—highlight and promote researcher engagement and, in the case of ECCSA, are willing to receive potential cybersecurity vulnerabilities that relate to any vendor in the aviation sector.[17] Additionally, in August 2019, the first-ever Aviation Village was held at the DEF CON hacker conference, which focused on building bridges and trusted partnerships between the aviation sector and good-faith researchers.[18]

All of these developments suggest that the building of such relationships may have turned the corner, and there is hope of increased cooperation between the research community and aviation sector.

## 5.2 CHALLENGES

Cyberattacks against aviation organizations appear to be increasing.[19] Although there is much industry focus on traditional information-technology (IT) systems for threats such as ransomware and theft of personally identifiable information (PII) or intellectual property, attacks on airport systems—like those that targeted flight-information displays at Odessa International Airport—are examples of adversarial evolution.[20] Additionally, the increased sophistication and scale of spoofing of Global Positioning System (GPS) signals, seen recently in the maritime domain, indicate how adversary techniques are rapidly evolving.

The cybersecurity and resiliency of Automatic Dependent Surveillance–Broadcast (ADS–B) have been discussed for many years. As a surveillance technology that uses GPS and position broadcasts to assist with situational awareness and separation, it is quickly becoming a cornerstone of the ATM system. But, challenges remain. Outages caused by either signal interruptions or spoofing could rapidly cause operational impacts. An example is that, in 2019, a short period of system errors across some ADS–B units caused about four hundred flights to be cancelled.[21]

Even these examples arguably belie the fragility of the situation. Combining the current levels of connectivity with increasingly technically capable adversaries, one can expect attempted widescale, disruptive future attacks against aviation operations. The first generation of these attacks will likely impact confidentiality of data or availability of systems. Such an attack against aviation systems with multiple backups and a workforce that trains for system failure will potentially still disrupt capacity or rate of operations, but likely not cause critical impacts. More concerning second-generation attacks against data integrity would be significantly more challenging to both identify and address. Adversary behavior in other sectors has indicated that adversaries dedicate themselves to learning about the systems they plan to attack; the aviation sector is no different. Even in a sector where humans are seen as the last link in the flight-safety chain, a compromise of the integrity of the information on which they rely to make safe decisions would cause significant challenges.

Arguably the most critical risk to the aviation sector—terrorism—was previously not considered through a cybersecurity lens, because kinetic effects were simpler to carry out, so long as the threat actor gained physical access. But, as increased physical security hardens and wireless connectivity increases throughout a multitude of aviation systems, there is a growing risk that aviation-cybersecurity vulnerabilities may become a credible vector for terrorist actors—either enablement of physical attacks or as an end goal in themselves. With this increased risk, international focus on the cybersecurity aspects of UNSCR 2341 and the protection of critical infrastructure against terrorist attacks has been increasing.[22] Dialogues between Interpol, the United Nations (UN), ICAO, and national bodies to counter terrorist activity across both the cyber and physical domains will likely become even more tightly woven.[23]

17 "Vulnerability Disclosure—Request for Assistance," European Centre for Cyber Security in Aviation, last visited November 19, 2019, https://www.easa.europa.eu/eccsa/eccsa-request-assistance-vulnerability-disclosure.

18 "Aviation Village," last visited November 19, 2019, https://aviationvillage.org/.

19 "Cyber Security in Aviation," Aviation Intelligence Unit, EuroControl, August 2019, https://www.eurocontrol.int/sites/default/files/2019-08/cybersecurity-in-aviation-eurocontrol-think-paper-3.pdf.

20 "'F*ck you": in Odessa, Hackers Staged a Cyber Attack, Airport Operation is Paralyzed," October 17, 2019, https://odesa.znaj.ua/ru/270882-f-ck-you-v-odesi-hakeri-vlashtuvali-kiberataku-robota-aeroportu-paralizovana.

21 Stan Goff, "U.S. Flights Canceled as FAA Looks into GPS, ADS-B System Errors," *Inside GNSS*, June 10, 2019, https://insidegnss.com/u-s-flights-canceled-as-faa-looks-into-gps-ads-b-system-errors/.

22 "Resolution 2341: Threats to International Peace and Security Caused by Terrorist Acts," United Nations Security Council, February 13, 2017, http://unscr.com/en/resolutions/2341.

23 "UNSCR 2341 and the Role of Civil Aviation in Protecting Critical Infrastructure from Terrorist Attacks," International Civil Aviation Organization, 2107, https://www.icao.int/Meetings/AVSEC2019/Pages/Critical-Infrastructure.aspx.

# 6: Report Findings and Analysis

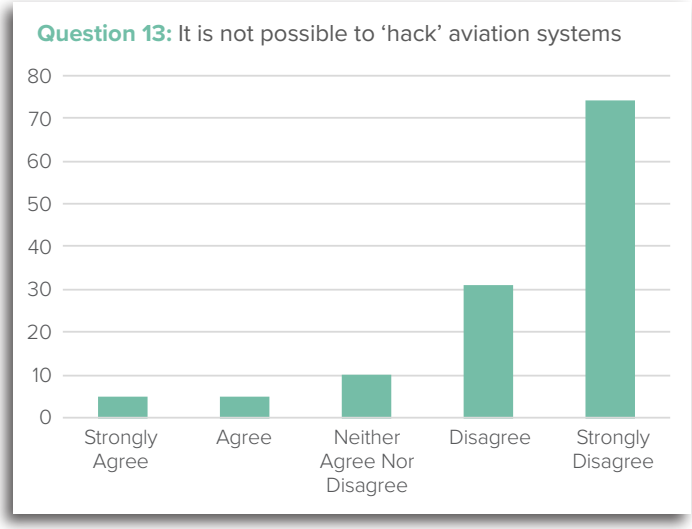
With the breadth, variety, and overlap of the cybersecurity challenges facing the aviation sector, it can be difficult to structure these challenges in a clear manner. Therefore, the report findings have been structured to flow through the challenges of managing aviation-cybersecurity risk, gaining insight into that risk, the management of potential aviation-cybersecurity incidents, and, finally, exploring the challenges of regulation, standards, and best practices that can manage and mitigate these risks.

## 6.1 MANAGING AVIATION-CYBERSECURITY RISK

Managing risk is a key challenge in cybersecurity. In safety, the aviation industry has, for many years, been focused on driving risk as low as reasonably practicable (ALARP). This has been achieved through the development of a strong safety culture, objective oversight, and rapid and robust information sharing. As a result, accident and incident rates have seen historic lows.

The digitized and connected aviation ecosystem includes such a high number of diverse actors, services, devices, and data that it is very difficult to map out a comprehensive view. This increasing attack surface and complexity have made managing aviation-cybersecurity risk a strategic challenge.

To manage risk, it is first necessary to identify and understand that risk. What became clear from the survey results, workshops, and interviews is that, for aviation cybersecurity, identifying and understanding risk remain critical challenges. A clear majority of respondents disagreed or strongly disagreed with the statement that it isn't possible to hack aviation systems. The new reality is that aviation systems are likely to face vulnerabilities and challenges similar to those of other sectors.




One respondent discussing their perspectives on the main blockers to improving aviation cybersecurity stated, "everyone believes that it is not vulnerable." Overall, respondents clearly disagreed with the statement that is "easy to objectively assess aviation security risk." This means that considerable effort is now required to improve the understanding of risk.

It is heartening that most respondents involved in aviation operations reported that their organizations had a cyber strategy in place to appropriately manage aviation-cybersecurity risk, but work remains to get this figure to 100 percent. Further discussion also highlighted the challenges between developing an enterprise cybersecurity strategy with one that also incorporated aviation-cybersecurity risk. With connectivity between operations and enterprise now increasingly difficult to separate, it is important to ensure that cyber strategies and accountability appropriately consider both aviation operations and the enterprise.

The challenge of having enough appropriately trained cybersecurity staff to manage cybersecurity risk is keenly felt across many sectors. From the results of the survey, the aviation sector faces the same challenge, but even more so, due to the need to develop a workforce with expertise in both aviation and cybersecurity. As momentum builds in generating aviation-cybersecurity capabilities, the challenge of finding and developing an aviation-cybersecurity-aware workforce will become more acute, and the sector will need to compete with others for talent.

With cybersecurity risk being subjective, it is crucial to consider what stakeholders perceive as an adequate baseline of cybersecurity risk management and transparency within products and services. Ultimately, transparency between supplier and customer promotes informed decision-making between both parties about the cybersecurity requirements and the cybersecurity status of the product or service. The question that explored this challenge asked respondents if they felt that cybersecurity requirements were transparent and agreed upon in aviation contracts; the response was a resounding no.

Following this, many respondents also disagreed with the statement that it "was easy to incorporate best practices into the procurement of aviation-related hardware, software, and services." There may be a number of reasons for this—and perhaps more clarity is needed on what exactly constitutes "best practices"—but this fundamentally points to the question of how much cybersecurity should be "built-in" versus "built-on" in the aviation sector. If aviation service providers are struggling to understand system-cybersecurity requirements

An airplane taking off at sunset

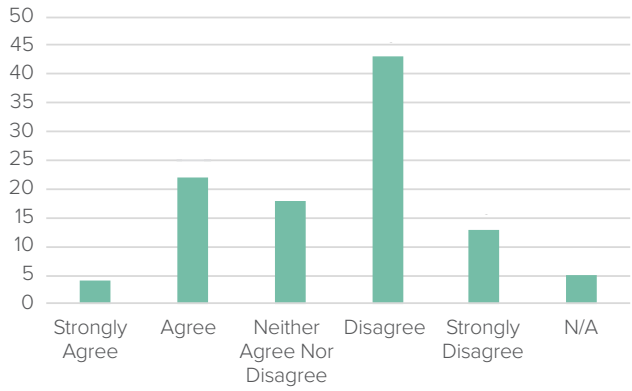
and best practices, a key requirement must be defining an adequate, minimum baseline of cybersecurity for the design of the product and service.

The previous two questions demonstrate that many respondents saw challenges in the cybersecurity dialogue between supplier and customer across the aviation sector, and this extended throughout the product lifecycle. With the lengthy lifecycle of many products in the aviation sector, and the potential for multiple ownership changes over the years, focus on "through-life" cybersecurity management will be critical if the sector is to adequately manage cybersecurity risk through the second- and third-hand markets until end of life and disposal.

Across the aviation sector, the amount of cybersecurity-relevant data being produced is expanding at an exponential rate. The ability to access and analyze such data, to gain significant insight and identify potential issues, is essential to managing risk. Between suppliers and customers, it is critical to understand how such data are provided and at what cost. From the survey results and discussions, respondents reported that there are blockers and potentially additional costs to accessing such data.

Overall, the results, comments, and discussions show both suppliers and customers across the aviation sector

**Question 49:** Throughout the passenger journey from airport to airport, the protections in place for their privacy and cybersecurity is adequate




## Passenger privacy and cybersecurity

With the rapid expansion of connected digital services available to passengers across their journey—ranging from biometric security to airport and aircraft services—passenger privacy and security are increasingly sensitive and critical topics. On the whole, respondents disagreed that current privacy and security protections were adequate. As evidenced in other sectors, a proactive approach and transparent dialogue with passengers on these topics create informed positions and increased trust.

have challenges in understanding and managing aviation-cybersecurity risk. None of these challenges is insurmountable, but they require increased dialogue within organizations managing aviation-cybersecurity risk, and between customers and suppliers of products, software, and services across the aviation sector. The more that cybersecurity is considered, discussed, and explored, the easier it will be to visualize—and, therefore, manage—the risk.

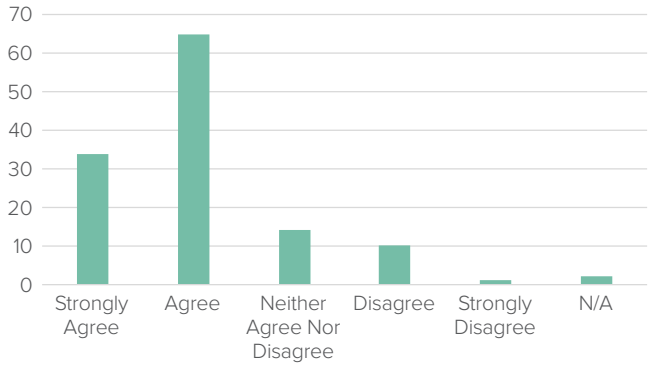
## 6.2 GAINING INSIGHT INTO AVIATION-CYBERSECURITY RISK

For aviation organizations to manage risk, they need to be able to gain insight and understanding of potential vulnerabilities, as well as to understand the threat. Complex platforms, systems hardware, software, and multiple service providers, alongside traditional enterprise structures and complex governance, including security and flight safety, can make developing such insight challenging.

With a comprehensive understanding of risk, management of that risk becomes considerably easier. From the responses received, it is clear that considerably more can and must be done to improve understanding of risk across the aviation sector.

The first survey question explored whether there was sufficient aviation-cybersecurity dialogue across stakeholders, and it became clear that respondents did not think this was the case. There is robust dialogue on the topic of safety globally, and across a multitude of stakeholders—for example, ICAO Regional Aviation Safety Groups and InfoShare events. This dialogue assists in the identification of potential risks and their mitigations. On aviation cybersecurity, it is essential that the sector generates, mirrors, and enshrines the same level of dialogue. This will not be easy; within flight safety, the focus is very much on finding the root cause and sharing it without blame. Across much of the cybersecurity landscape, there arguably remains a stigma about discussing cybersecurity vulnerabilities and challenges that go beyond managing sensitive vulnerabilities. The aviation sector must actively work to improve and mature the current culture.

**Question 12:** The use of approved, independent companies to objectively assess the cybersecurity of aviation products and services is useful to gain insight to risk



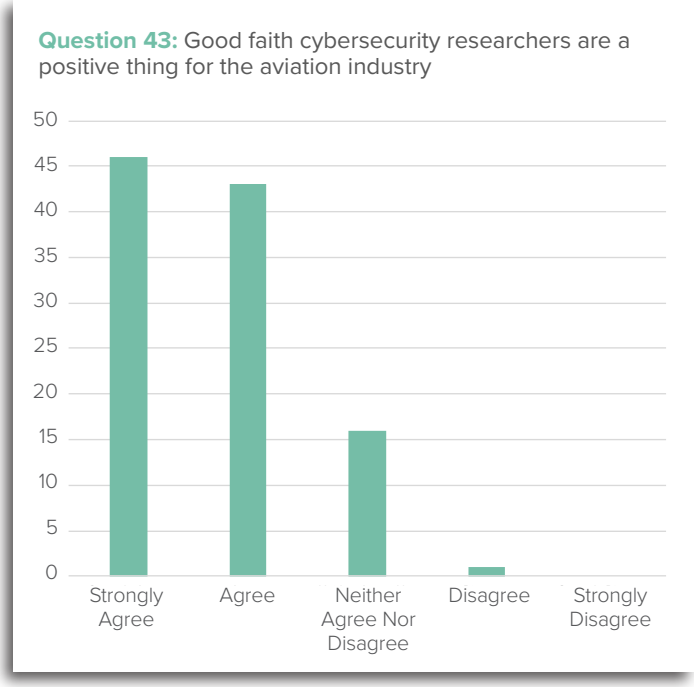

The use of independent, objective assessments to determine the safety of aviation products and services is well established. It is clear from the survey findings that this approach is equally desired when it comes to assessing and gaining insight to cybersecurity risk in the aviation sector. The use of Coordinated Vulnerability Programs (CVP) has proven highly successful in discovering previously unknown vulnerabilities. It is encouraging to see around 50 percent of respondents say that their organization has a CVP program in place, but much work remains. One respondent reported that, from their perspective, "a lack of a coordinated vulnerability disclosure culture among the private and public organizations involved in civil aviation" was the main blocker to improving aviation cybersecurity.

When raising the topic of bug-bounty programs (in which an organization motivates individuals to report potential cyber issues and vulnerabilities with the offer of financial rewards), it is fair to say that their use is not widespread across the aviation industry. Bug bounty programs, as an element of a mature cybersecurity strategy, have considerable benefits, as demonstrated by the multiple vulnerabilities found by programs such as Hack the Air Force and Hack the Pentagon.[24]

Within the ICAO cybersecurity strategy, "states are encouraged to set up appropriate mechanisms for cooperation with good faith security research—research activity carried out in an environment designed to avoid affecting the safety, security and continuity of civil aviation."[25] This change should globally help drive positive and productive engagements between the aviation industry and security researchers. From the results of the survey and workshops, respondents thought that such cooperation is a positive development for the aviation sector. Conversely, many respondents did not agree that sufficient advice and guidance were available for good-faith researchers who want to research aviation cybersecurity in a safe manner, or that they had adequate and well-understood legal protections in place. The perceived difficulty that good-faith cybersecurity researchers face when contacting companies within the aviation sector also contrasts with the results that point to organizations firmly welcoming such approaches. If the aviation sector can create and promote clearer and easier processes

24 "USAF Announces Hack the Air Force 3.0," US Air Force, November 5, 2018, https://www.af.mil/News/Article-Display/Article/1682502/usaf-announces-hack-the-air-force-30/; "Department of Defense Expands 'Hack the Pentagon' Crowdsourced Digital," US Department of Defense, October 24, 2018, https://www.defense.gov/Newsroom/Releases/Release/Article/1671231/department-of-defense-expands-hack-the-pentagon-crowdsourced-digital-defense-pr/.

25 "Aviation Cybersecurity Strategy," Aviation Civil Aviation Organization.





The International Civil Aviation Organization (ICAO) headquarters in Montreal, Canada

for researchers to work with them, it is obvious that there is great benefit to be had for both stakeholder groups. These new processes also have the potential to create increasingly positive interactions between good-faith researchers and the aviation industry.

## 6.3 AVIATION-CYBERSECURITY INCIDENT MANAGEMENT

Irrespective of the effort put into preventing accidents or incidents, the aviation industry fully understands that accidents and incidents still occur. Years of hard-won experience and development of best practices have resulted in globally agreed-upon rules and regulations that ensure robust and objective investigation, with the goal of never suffering the same accident or incident twice.

To deal with flight-safety incidents, there is a clear and well-understood process. With digitized and connected systems now underpinning operational safety, understanding how to prepare for, identify, manage, and learn from aviation-cybersecurity incidents will be critical.

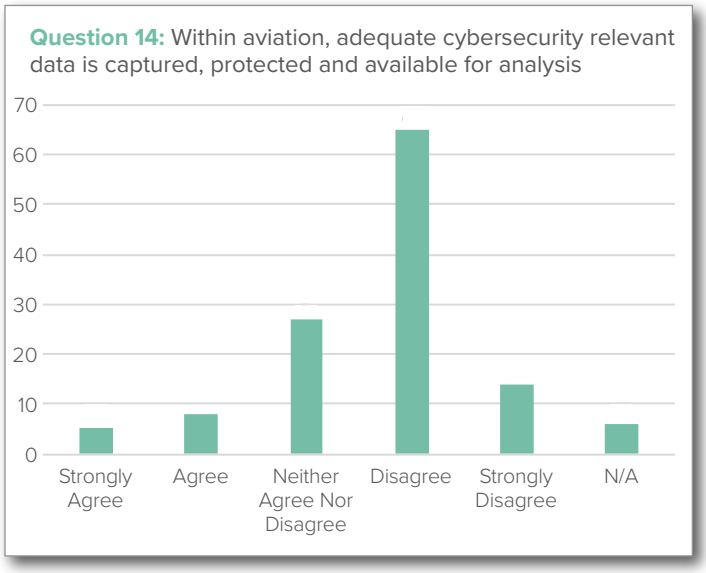
To the initial question of whether they thought the organization was well prepared for aviation-security incidents, respondents felt their organizations were, on the whole, prepared. However, the subsequent questions highlighted some challenging nuances between the management of safety and security incidents and aviation-cybersecurity incidents.

With the increasing awareness on the topic, it would be difficult to find an organization that didn't have a degree of cybersecurity-awareness training. The aviation sector is no different, with the majority of respondents saying that all staff received such training. But, when taking that question forward to explore whether their organization had appropriate cybersecurity culture in place, considerably fewer respondents thought that was the case. Historically, flight-safety-and-security culture has achieved considerable results for the aviation sector. With the importance of a cybersecurity culture clearly stated in the new ICAO Cybersecurity Strategy, this area will need considerable attention. As part of this effort, developing a clear understanding of aviation-cybersecurity culture, and its interplay between flight-safety culture and security culture, will be critical.

With aviation cybersecurity straddling both safety and security, a consistent solution to its governance and accountability has yet to be developed. This challenge is brought into stark focus during the management of an aviation-cybersecurity incident. Currently, many aviation organizations split cybersecurity-incident responsibilities between networks (traditional enterprise) run by the chief information security officer (CISO), and products (aircraft, operations, etc.) run by the safety team. The fact that, even with current levels of connectivity, such a division of responsibilities is arguably unrealistic was strongly reinforced. One contributor explained that the "safety committee may own the plane, but they have no cybersecurity expertise." It was suggested that a more robust approach that better aligns responsibilities to the reality of the networks would require considerable cultural change. With the majority of survey respondents believing that an incident response would be led by a joint team, there is much room to improve and adjust existing organizational processes. Another contributor described the "ongoing separation of safety and cybersecurity within the industry" as the main blocker to improving aviation cybersecurity and resilience. Ultimately, there is much work to be done to develop the governance and processes around such organizational structures, but the benefits could be considerable.

For years, the human operator has always been seen as the critical link in the flight-safety chain, as he or she is able to recognize and prevent flight-safety incidents. With connected, digitized technology now underpinning safety-critical systems, there is now a risk of adversaries undermining that critical safety break. The two questions exploring whether operational staff was trained to both recognize and manage a potential aviation-cybersecurity incident did not give clear answers, potentially because such a situation has yet to occur. Research by EASA carried out in 2016 used a flight simulator to assess the potential safety impacts of cyberattacks on aircrew.[26] The results demonstrated that it was challenging for the crews to recognize such attacks, but, if standard flight-operation practices were followed, safety issues could be mitigated. Efforts must be made to expand this research to provide practical advice that can be woven into role-based training for aviation operators.

Rigorous training is a cornerstone of developing aviation operators who can deal with whatever is thrown at them, in order to maintain safe operations. From responses to the question on the conduct of exercises relating to aviation-cybersecurity incidents, it is clear that such exercises are not yet common. There is hope that this situation will improve soon, as preparing for aviation-cybersecurity incidents does not just train operators, but also helps build organizational understanding and maturity in dealing with such incidents.




The aviation sector, with its objective of never suffering the same accident twice, has a rigorous and objective incident-investigation methodology that will explore both the root technical causes and the organizational, systemic causes. With increased digitization of all systems within the aviation sector, the complexity of data, ownership, and governance now presents a significant challenge to investigating potential cybersecurity aspects of accidents and incidents. Results clearly indicate that respondents do not believe that adequate cybersecurity relevant data are captured, protected, and available for analysis. Additionally, in learning from other sectors and advanced threat-actor techniques, simply capturing data is not enough; data capture must be rigorously protected from interference. In order to frustrate and disrupt cybersecurity investigations, cyber threat actors will compromise the integrity and availability of data and security logs relevant to the investigation and remediation. Therefore, it must be acknowledged that simply capturing such data will not be enough; data must be adequately protected and accessible.

26 "Impact Assessment of Cybersecurity Threats (IACT): EASA_REP_RESEA_2016_1," European Union Aviation Safety Agency, July 31, 2018, https://www.easa.europa.eu/document-library/research-reports/easarepresea20161.

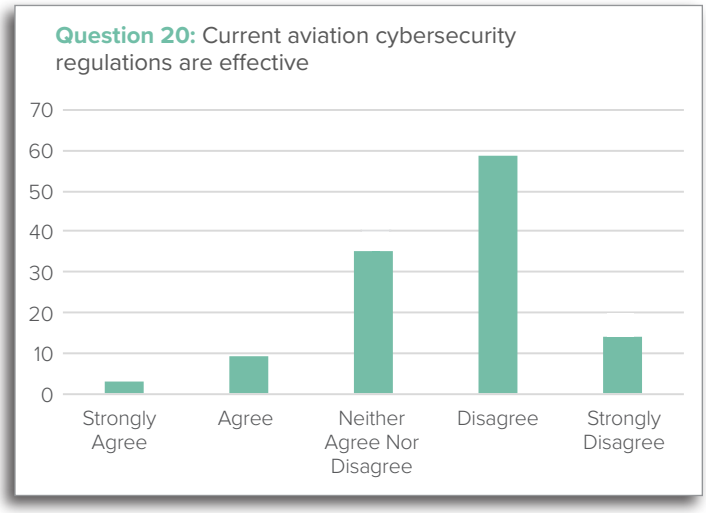
Finally, how organizations manage communications around any incident or accident is crucial. Currently, respondents do not think that the aviation sector effectively communicates about aviation cybersecurity with external stakeholders. With the added pressure of managing an aviation-cybersecurity incident, it would be very clear that there is much to be done to increase effective communications and build understanding across stakeholders and the media.

## 6.4 REGULATIONS, STANDARDS, AND BEST PRACTICES

With the cybersecurity challenges the aviation industry faces, regulations, standards, and the development of best practices are, and will continue to be, a cornerstone for systemically understanding and reducing risk at a global scale. This section explores contributor perspectives across this important topic.

Regulations and standards have been, and will remain, critical components of a safe, efficient, and harmonized global aviation industry. To the question of whether respondents perceived current aviation-cybersecurity regulations as effective, clear, and well understood or well communicated, the responses indicate they are not. It could be easy to conclude that more regulation is the answer; however, there is a need to find a balance. Excessive regulations and standards can slow growth and innovation, while too few can result in technical divergence and little understanding of the creation of systemic risk. As seen with cybersecurity in other sectors, like finance or power generation, heavy regulation without balance can lead to a compliance culture, especially at board level—chasing yearly audit goals for shareholder reports. Efforts must be made to find a balanced regulatory approach for the aviation sector that promotes good behavior and an appropriate culture to manage aviation-cybersecurity risk.

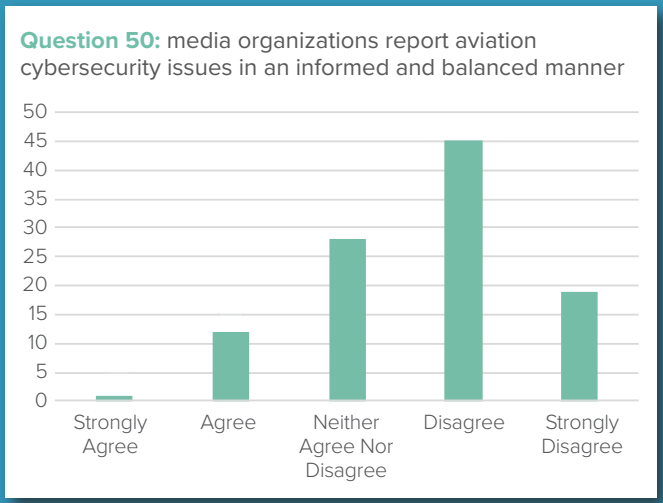
In minimizing risk, aviation already has an effective model in flight safety, where there is never enough effort, and risk is always being driven down. Therefore, aviation-cybersecurity regulations and standards must not be seen as a minimum to be achieved, but as measures that sit alongside a culture of cybersecurity, driven by senior leadership and spread throughout the organization.




There is a clear contributor perception that aviation-cybersecurity regulation should be led globally, placing ICAO in a strong leadership position. To maximize this position and accelerate progress in an increasingly crowded international field, ICAO will need to take on this role with the strong support of its members and the aviation sector. Such an approach would create an environment for global coherency across aviation-cybersecurity regulations, as well as the internationally agreed-upon best practices desired by all stakeholders.

Respondents were asked where they look for advice on aviation cybersecurity, and it is clear that industry bodies, government departments, regulators, and vendors have roles in that advisory capacity. Respondents felt only somewhat supported

### Aviation cybersecurity and communications




As part of normal business—and especially during any cybersecurity incident—effective and clear communication is essential to help manage and mitigate loss. For many stakeholders, aviation cybersecurity has been a challenging topic to discuss with external stakeholders, such as the media.

It was suggested that, on the topic of aviation cybersecurity, the media "have struggled to find enough best practice examples and so have generally not been able to write about the issue with any purpose." If the dialogue on aviation cybersecurity is to be balanced and informed, the aviation industry must be open to discussing ongoing efforts and realistic challenges.

by these stakeholder groups. A follow-on question about how satisfied respondents were with their ability to access advice on aviation-cybersecurity best practices and guidance showed a large degree of dissatisfaction; overall, there is much to be done. At this stage—with increased focus on aviation cybersecurity, and the rush to further develop regional and national regulations, standards, and best practices, there is also a critical risk of divergence. With the new ICAO Cybersecurity Strategy (and the associated action plan, which at the time of this report's publication is under development), the updated DO-326, and ED-202, there is potential for a structured global effort that can also apply to the appropriate organizations. Too many standard-setting bodies or proffered best practices risk incoherency and complexity.

All of this makes future investment in cybersecurity critical. Though many of the respondents agreed that their organizations plan to invest more in aviation cybersecurity, the question remains: invest in what? It has become clear that confusion remains about aviation-cybersecurity standards, regulations, and best practices. For organizations willing to spend more money in this area, it is challenging to make informed decisions. Arguably, this area is underserved from a commercial perspective, with a sectorial desire for improvement and additional budget overhead. The critical challenge will be ensuring not just the creation of an aviation-cybersecurity support industry, but one that supports the aviation industry in synergy with its current strengths. Much like a technical solution in isolation is never the answer to flight safety, it is also not the answer to aviation cybersecurity. Improving aviation cybersecurity must be approached holistically—across people, processes, and technology—and in synergy with already-robust safety culture and current aviation best practices.

# 7: Conclusions

It is clear from the survey results, workshops, and interviews that, although the aviation sector continues to have multiple and critical cybersecurity challenges, progress is being made in understanding and managing them. The diversity of voices and perspectives remains, but that should not be interpreted as a negative thing. Strength lies in diversity, and the challenge is finding a way to work together through that diversity. From an adversary's perspective, the burgeoning cyberattack surface presented by increased digitization and connectivity, stretching from land to space, makes it both an attractive target for and an enabler of adversary action.

## 7.1 MANAGING RISK

A key element of cybersecurity is accepting the reality that vulnerabilities exist, proactively identifying them, and then fixing them before they can be exploited by adversaries. Achieving this requires acceptance, management, and organizational processes, just as much as technical capability. It is clear from the report contributions that cybersecurity vulnerabilities and risks exist in the aviation sector. With flight safety, the aviation sector demonstrably has the right mindset in managing risk. Now it must apply this mindset to managing the reality of its cybersecurity challenges.

Although progress is being made, a key theme brought up by many contributors to this report is a perceived lack of knowledge, understanding, and leadership in tackling what is now a critical aviation-cybersecurity challenge. To move forward and overcome inertia will require significant leadership from international organizations, governments, and industry, which must raise awareness of the critical nature of the challenge, tangible mitigations, and efforts under way. Even the simple step of highlighting where organizations can start on their aviation-cybersecurity journey will help—especially as this is a multinational issue with diverse starting points.

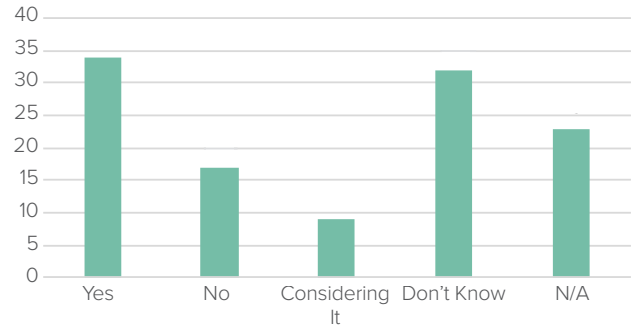
Many sectors have silos across which governance, accountability, and management of risk prove difficult, and the aviation sector is no different. For years, flight safety and security have evolved into effective, but understandably separate, elements within the aviation sector. Across aviation cybersecurity and enterprise IT, the collaboration between all these elements will be challenging, but is at the heart of future success.

The importance of proactive cybersecurity management and transparency throughout the lifecycle of aviation products, services, and software is critical. It cannot be considered with only the first buyer in mind, but must also consider the second, third, and fourth users, as well as end of life and disposal. This

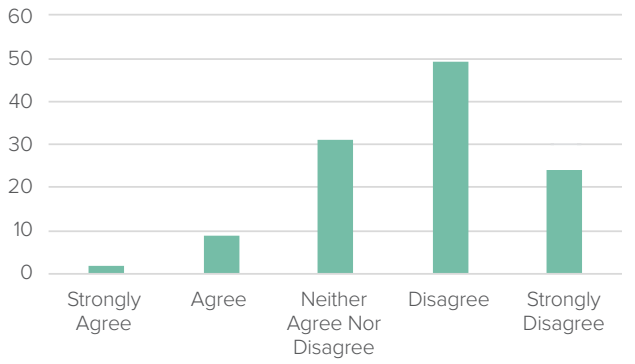
### The role and challenge of cyber insurance

There is an increasing market for cyber insurance as companies incorporate it as an element of risk management. These two questions explored whether respondents' organizations included cyber insurance as an element of managing their aviation-cybersecurity risk. The next question explores their perspective on how easily they believed insurance underwriters could assess that risk. It is clear that, although there is significant usage of cyber insurance in aviation, assessing the risk exposure is challenging. Managing the dichotomy of increasing coverage with a potentially limited understanding of risk will require increased collaboration between underwriters, insurers, and the insured.

**Question 31:** Our organization includes cyber insurance as an element of managing our aviation cybersecurity risk




**Question 32:** It is easy for insurance underwriters to assess aviation cybersecurity risk



will need both suppliers (original equipment manufacturers (OEM) or other) and customers to incorporate such thinking into contractual agreements, so that risks and their management are accounted for and transparent.

Managing aviation-cybersecurity risk across such a complex system is challenging. Some of this challenge may be due to organizational issues, but much of it also lays with system design/architecture, and the issue of gaining objective insight into risks. For flight-safety critical systems, objectively and independently testing them for assurance is the norm. Embracing this cultural approach across digitized and connected systems should be seen as a standard methodology in managing aviation-cybersecurity risk, whether it is conducted by the OEM, the end user, or the regulator.

At every step of aviation-system design, building, manufacturing, and operation, cyber-secure and resilient-by-design must be the default for every process, along with strenuous efforts to minimize attack surface. Such system design must also enable operators to quickly restore systems to airworthiness after a compromise (or test). Additionally, with a considerable number of legacy systems already in use, efforts must be made to fully understand their potential attack surface and develop mitigations for existing systems.

In the tumult and excitement of rapid technological innovation, considerations around the privacy and cybersecurity of passengers cannot be forgotten. Other sectors have learned the hard way about losing consumer trust through poor transparency or security, alongside compliance frameworks that reactively change due to consumer pressure. To maintain consumer trust, there must be an informed and transparent dialogue about consumer data and privacy, encompassing everything from the increased use of biometrics for security, airborne Wi-Fi, and the use of cameras both on the ground and in the air.

Finally, it will not be possible to manage aviation-cybersecurity risk without personnel who can meet the challenge. Achieving this across the aviation sector will require a great deal of skills diversity, going beyond technology into policy and strategy, and crossing multiple stakeholder groups.

## 7.2 GAINING INSIGHT INTO RISK

Contributors to the report strongly believe that aviation-cybersecurity risks exist, and that actively identifying risks and preparing for their potential realization are critical.

To achieve this, there must be increased dialogue and contributions from all aviation-sector stakeholders, including manufacturers, end users, governments, and regulators. As part of this dialogue, there must be a willingness to hear different perspectives on risk, test assumptions, and be unafraid of what might be found. Wherever possible, this learning must also be collective, with stakeholders sharing hard-earned aviation-cybersecurity knowledge and best practices as if they were flight-safety-critical information, rather than cybersecurity information.

Even outside the aviation sector, there are relevant potential challenges for how cybersecurity vulnerabilities are shared and actioned. In the ongoing class-action suit *FCA US LLC v. Flynn*, consumer (customer) plaintiffs claim that a manufacturer knew of, but did not fix, a cybersecurity vulnerability. The plaintiffs allege an overpayment theory; that is, had the plaintiffs known about the vulnerability, they would not have paid as much or bought the product at all.[27] Until this suit is settled, there is a risk that vulnerability disclosure and management will become increasingly limited, when they should be increasing in transparency and collaboration. To overcome these challenges, partnerships must develop between all stakeholders focused on minimizing risk, rather than legal jeopardy, as the priority.

Achieving this will require a cultural shift. Wherever there is a requirement for a flight-safety or security culture, there must also be an aviation-cybersecurity culture that stretches from supply chain to operator. Once achieved, this will drive improvement across the sector, from passive and reactive to positive and proactive

## 7.3 INCIDENT MANAGEMENT

Adversaries will exploit organizational boundaries, utilizing confusion and miscommunication as means of obscuring or amplifying their attack. In flight safety, the aviation sector has a proven model of how good leadership, governance, accountability, information sharing, and safety culture can make a significant difference in reducing risk. The sector must strive for the same model regarding cybersecurity.

Recognizing and responding to cyberattacks within the aviation sector is a whole-of-sector responsibility. The nature of the potential attacks is such that the frontline of aviation cyber defense stretches internationally across service-provider personnel including pilots, air-traffic controllers, maintainers, security-operations centers (SOC), contractors, and more.

27 Megan L. Brown and Boyd Garriott, "Supreme Court Declines Connected Vehicle Lawsuit, Leaving Standing Issues in Tech and Security for Future Resolution," Federalist Society, February 4, 2019, https://fedsoc.org/commentary/blog-posts/supreme-court-declines-connected-vehicle-lawsuit-leaving-standing-issues-in-tech-and-security-for-future-resolution.

Therefore, all the personnel in this chain must be trained to recognize and manage potential cyber incidents. This must not be seen as an opportunity for system design that pushes responsibility for cybersecurity to the end user or service provider. Inherent system design should focus on making systems secure and resilient, with the end user, irrespective of their role, as protected as possible in their need to make safe and timely decisions.

There must also be an industry-wide assessment of the cybersecurity investigatory aspects of post-accident and post-incident investigations. This must be led in partnership with post-crash-investigation (PCI) bodies, with findings subsequently incorporated into industry best practices. This may also highlight gaps in how relevant aviation-cybersecurity data are collected and protected, and these findings must be fed back into standards, manufacturers, and operators.

Following a cybersecurity incident or exercise, returning aircraft to a safe and flying state must be as efficient and safe as possible. Much of current practice is to replace hardware in the event of software issues. But, in the event of a widescale incident, such an approach may slow progress in restoring full operational capabilities, especially at scale. Finding a way to improve this must be a priority for the sector—not just on aircraft, but across all operations, including ATM. To improve resilience, the sector needs plans that prevent critical failure, but also minimize impacts, restore full operations as soon as possible, and rebuild trust.

## 7.4 REGULATIONS, STANDARDS, AND BEST PRACTICES

Regulations and standards exist for aviation cybersecurity, and considerable effort has been put into creating them. Nevertheless, somewhere along the line, there has been a disconnect resulting in significant contributors disagreeing with the effectiveness, clarity, and communication on these regulations and standards. This situation may improve with the updated DO-326 and ED-202 documents, but changing current perceptions will likely take considerable effort. It was made very clear during the workshops that the bodies writing such standards were keen for input from across the whole sector. This is not just a case of increasing awareness of standards, but also increasing collaboration on them.

For organizations in a technical industry looking to manage their cybersecurity risk, there will be a strong temptation to reach for technical solutions, and understandably so. The analogy to this is that flight-safety success does not come through technical solutions in isolation. It is more a matter of how people, processes, technology, and culture are woven together that brings success; aviation cybersecurity must be approached in the same manner.

As a global sector, aviation absolutely depends on global coherency for interoperability, collective understanding of risk, efficiencies, and considerably more. Varied standards, best practices, and complex demands on the supply chain will increase costs for all parties, as well as make it considerably harder to coherently understand risk. Having an international body such as ICAO brings the leadership and ability to maintain that coherency. Respondents see that leadership role as crucial, especially when considering the initiatives on aviation cybersecurity across multiple regions; there are risks that this global coherency could be compromised. A concerted effort will be required to bring coherent global, regional, and national structure to aviation-cybersecurity regulation and best practice. A balance must be found between regulation and culture, as burdensome regulation could create a compliance culture that undermines the principles and culture of flight safety, which is continually striving to drive risk down.

Finally, a structured approach to aviation cybersecurity—either through regulations or standards—enables the development of aviation-cybersecurity roles and qualifications that will promote the building of a critically needed workforce. Until the sector can define such roles and qualifications, the building of a global aviation-cybersecurity workforce will be based more on luck than structured planning. The roles within this workforce cannot be purely technical; they must be created with depth through the critical non-technical roles, such as policy and strategy.

There is no single solution, role, or action to solve aviation-cybersecurity challenges. It will require a collaborative and proactive effort to develop the right regulations, standards, and best practices across this global industry. Even with clear leadership, this task will be a challenge—but it *is* possible.

# 8: Suggested Next Actions

## This report recommends the following next steps for the aviation ecosystem

### 8.1 Global standards for a global industry

With publication of the ICAO Cybersecurity Strategy, there is now a vision for how aviation cybersecurity can advance globally.

"ICAO's vision for global cybersecurity is that the civil aviation sector is resilient to cyber-attacks and remains safe and trusted globally, whilst continuing to innovate and grow."[28]

To coherently gain insight, understand and manage aviation-cybersecurity risk, and bring swift, globally aligned, and effective change, all aviation stakeholders—including states, international bodies, regulators, manufacturers, and service providers—are strongly encouraged to act in unison and support the new ICAO Cybersecurity Strategy, as called for through the ICAO Assembly Resolutions A40-10 *Addressing Cybersecurity in Civil Aviation*.

### 8.2 Increasing transparency and trust

Trust in aviation cybersecurity will only come with increased transparency. Limited or ineffectual information sharing is leading to opacity of risk among stakeholders, and arguably obfuscates the scale of the aviation-cybersecurity challenge and the way forward. Actions to improve this fall into two key areas.

#### 8.2.1 Contracts

All contracts between aviation stakeholders must include cybersecurity considerations, such as through-life risk management, vulnerability management, and data sharing. These must be clearly and transparently agreed upon, to ensure that all stakeholders are able to make informed decisions on cybersecurity risk.

#### 8.2.2 System design

Aviation-system design must be approached from the perspective of not only securing systems, but also increasing cybersecurity risk transparency and objectivity for both manufacturer and customer. All stakeholders must be able to access and analyze their cybersecurity-relevant data. Additionally, efforts must be taken to reduce the rapidly expanding digital attack surface of the aviation sector, with a default of designing for simplicity, security, and resiliency—not complexity.

### 8.3 Building bridges

The scale and complexity of the cybersecurity challenge facing the industry is such that all stakeholders must be encouraged to support and learn from each other. There are three key areas.

#### 8.3.1 Diverse stakeholders

The scale, nature, and variety of the aviation sector is such that there are a number of diverse stakeholder groups that can productively collaborate to help understand and manage risk. Creating a rich and positive dialogue, including those from other sectors and cybersecurity researchers, will accelerate both the understanding of the challenge and potential solutions.

#### 8.3.2 Regulations and standards

ICAO, states, and standards bodies must be supported in the creation of informed and balanced aviation-cybersecurity regulations through input from diverse stakeholders, as a collaborative and structured effort to promote global coherency.

#### 8.3.3 Safety, security, enterprise cybersecurity, and aviation cybersecurity

Where aviation cybersecurity crosses the traditional elements of aviation security, safety, and enterprise IT, efforts must be made to break down silos and create a shared vision of risk.

### 8.4 Information sharing

Cybersecurity information sharing must be approached in the same way as information sharing on the topic of flight safety. Moving to a "learn once, share widely" model will promote rapid visibility, mitigation, and management of risk across the entire sector. Blockers to information sharing on aviation cybersecurity must be critically assessed, and standards must promote the sharing of cybersecurity-relevant information in a timely and responsive manner that gets defenders ahead of vulnerabilities and adversaries.

### 8.5 Communications

Aviation cybersecurity is a critical and complex topic that is still little discussed outside the sector, leading to risks of misperception and inaccuracy. Increasing external dialogue on the topic, and helping create informed positions, will go a considerable way to increase understanding and trust across multiple stakeholders.

28 "Aviation Cybersecurity Strategy," Aviation Civil Aviation Organization.

Flight taking off from Queen Alia International Airport in Zizya, Jordan

## 8.6 People

The global scale of the aviation-cybersecurity challenge means that it now touches every single element of the sector. Already, the sector does not have enough cybersecurity staff, and this shortage will only become more acute as initiatives and efforts increase. Global, sector-wide, coordinated efforts must be made to increase the cybersecurity skills of those already in the sector, as well as creating pathways and incentives for those wanting to embark on an aviation-cybersecurity career.

## 8.7 Passenger privacy and cybersecurity

How the aviation sector protects passenger privacy and cybersecurity must be a proactive and transparent dialogue. Starting discussions now on the topic of passenger privacy and security will also make it easier to develop appropriate supporting frameworks, reduce noncompliance risks, and scale technology such as biometrics.

# 9: Final Thoughts

The intent of this report was to explore multiple perspectives on the nature of the cybersecurity challenges facing the global aviation sector. It found that, although a multitude of perspectives remain, there is hope for—and some progress toward—building a shared understanding of aviation-cybersecurity risk.

With increasing digitization and connectivity, adversaries have significant attack surface and opportunity. The growing complexity of systems, process, and supply chain, alongside increasing wireless connectivity, adds to the potential weakening of the physical controls that have protected the aviation sector for so long. Combined with increasingly capable threat actors, ranging from terrorists to nation states, that means the aviation sector faces a significant task.

Where possible, the sector must seek quick wins, but also acknowledge that the challenge of securing the aviation sector from cyber adversaries is now a persistent problem. Therefore, the sector must be prepared to tackle large, systemic challenges, even if they are global in scale and will take considerable time to change. ICAO must be seen as the global lead on this topic—and it now has the strategy to deliver tangible change. It cannot drive change in isolation, and will require assistance and cooperation from states, industry bodies, and those contributing to the aviation sector if change is to be effective and long lasting.

Although progress is being made, significant challenges remain to both gaining insight into aviation-cybersecurity risk and globally managing it. Cultural change to better position the aviation industry to manage these cybersecurity challenges will take leadership and time. Measures must be taken to accelerate this process of improvement, increasing transparency and trust, and develop objectivity and collaboration.

There is no single solution to aviation cybersecurity, and it will take positive collaboration across diverse stakeholders. Building partnerships across safety, security, cybersecurity, and enterprise IT will also be challenging, but will lead to greatly increased understanding of holistic risk, better reflecting the nature of the complex attack surface being defended.

Along with all this effort, it must be remembered that the aviation sector is a global one, in which national and regional maturity and capability vary. Improving aviation cybersecurity will be a journey, and bringing along all stakeholders is essential if global, systemic risk is to be reduced. ICAO promotes this from a capacity-building perspective, with a tagline of “No Country Left Behind.” As global aviation-cybersecurity efforts ramp up, adopting the tagline of “No Vulnerability Left Behind” is a fitting update that describes where and how focus must be applied if the sector is to remain safe, secure, and resilient.

# Annex
# Survey Questions and Results

## 9.1 MANAGING RISK

Fundamentally, cybersecurity is about managing risk. In safety, the aviation industry has, over many years, driven risk to ALARP. It has done this through building a strong safety culture, objective oversight, and rapid and robust information sharing; the result has been historically low accident and incident rates.

But, with a digitized and connected aviation industry, it is easier to say what isn't connected than what is. Because of this increasing attack surface and complexity, managing aviation-cybersecurity risk was repeatedly raised as a key challenge. This first section explores the findings.

### 9.1.1 Questions 11 and 13
### Assessing aviation cybersecurity risk

One of the early questions explored if it was easy to objectively assess aviation-cybersecurity risk. Allied to this challenge was a question about whether respondents considered it possible to hack aviation systems. The genesis of this question was that during the research for the 2017 paper, Finding Lift, Minimizing Drag, one perspective offered was that it "wasn't possible to hack aviation systems."

### 9.1.2 Question 8
### Strategy

Respondents were asked if their organization had a cyber strategy in place to appropriately manage aviation-cybersecurity risk. This result shows only respondents from operational aviation organizations.

### 9.1.3 Question 37
### People to manage cybersecurity?

With many other sectors struggling with cybersecurity recruiting, this question reflected that challenge for the aviation sector.

### 9.1.4 Question 38
### Adequate cybersecurity as a standard?

To reduce cybersecurity risk at scale, an understanding must be developed in terms of what end users consider adequate baseline cybersecurity for products and services. This question explored adequate cybersecurity from an individual perspective.

### 9.1.5 Question 39
### Cybersecurity and product lifecycle

With aviation equipment in service for many years, this question explored perspectives around cybersecurity through products' entire lives.

### 9.1.6 Question 40
### Cybersecurity risk management between supplier and customer in aviation-related contracts

Within aviation, the relationship between customer and supplier is critical for understanding and managing cybersecurity risk. This question explored perspectives around aviation-related contracts, cybersecurity risk management, and transparency.

### 9.1.7 Question 41
### Incorporating cybersecurity best practices into purchasing aviation-related hardware, software, and services

Following on from the risk-management question, this question explored how easy respondents thought it was to incorporate cybersecurity best practices when purchasing equipment, software, and services.

### 9.1.8 Question 42
### Suppliers of products or services into the aviation sector provide cybersecurity-relevant data at no additional cost

Cybersecurity-relevant data allow for clear analysis both before and after incidents; this question explored if provision of this data was at an additional cost.

#### 9.1.9 Question 49

#### Passenger privacy and cybersecurity

With the rapid expansion of connected digital services to passengers across the whole of their journey—ranging from biometric security to airport and aircraft services—passenger privacy and security are increasingly critical topics. On the whole, respondents disagreed that the protections currently in place were adequate.

## 9.2 GAINING INSIGHT INTO AVIATION-CYBERSECURITY RISK

For aviation organizations to manage risk, they need to be able to gain insight into and understanding of potential vulnerabilities, as well as understand the threat. With complex platforms, systems hardware, software, and multiple service providers alongside traditional enterprise structures and complex governance, including safety, security, and flight safety, developing such insight is challenging.

This section explored some of the opportunities and challenges that aviation organizations face when gaining insight into risk.

#### 9.2.1 Question 30

#### There is sufficient aviation-cybersecurity dialogue between aviation-sector stakeholders

On topics such as flight safety and physical security, aviation-sector stakeholders have a robust, proactive, and effective dialogue on challenging issues. This question explored the often-discussed challenge of creating sufficient dialogue between aviation-sector stakeholders on the topic of cybersecurity.

#### 9.2.2 Question 12

#### Objectively assessing the cybersecurity of aviation products and services to gain insight into risk

This question asked respondents their perspective on the use of approved independent companies to objectively assess the cybersecurity of aviation products and services to gain insight into risk.

#### 9.2.3 Questions 24 and 25

#### The use of CVP and bug-bounty programs

The use of CVP and bug-bounty programs is increasing across many sectors, as a way to help find previously unknown vulnerabilities. This question explored their adoption in the aviation industry.

#### 9.2.4 Question 43

#### Researchers

During the research for the 2017 report Finding Lift, Minimizing Drag, the relationship between the aviation industry and the research community could be described as strained. There were likely several factors behind this. But, fundamentally, the tensions between those stakeholder groups were holding back potentially valuable contributions and collaborations in managing aviation-security risk. With the inaugural ICAO Aviation Cybersecurity Strategy specifically encouraging states to ensure adequate protection for good-faith security researchers, there is now a global imperative to improve relations and engagement between these stakeholder groups.

The first question on this topic explored whether the respondents thought that good-faith security researchers were a positive thing for the aviation industry.

#### 9.2.5 Question 44

#### Advice and guidance for good-faith researchers who want to research aviation cybersecurity in a safe manner

For good-faith researchers and the aviation sector to build trust and productive engagements, being able to understand how to work together will be critical. This question explored if the respondents thought there were enough advice and guidance for good-faith researchers to research aviation cybersecurity in a safe manner.

#### 9.2.6 Question 45

#### Good-faith cybersecurity researchers have adequate and well-understood legal protections in place

With increasing interactions between good-faith security researchers and the aviation sector, there has been increasing focus on the legal frameworks that support such activity. This question explored whether respondents believed that there were adequate and well-understood legal protections in place for such activity.

#### 9.2.7 Question 46

#### If they wish to disclose a potential vulnerability, it is easy for good-faith cybersecurity researchers to contact companies within the aviation sector

Previous research and interviews had highlighted potential challenges for researchers attempting to disclose potential vulnerabilities to organizations within the aviation sector. This question explored perspectives around how easy the respondents thought it was for researchers to contact companies within the aviation sector.

#### 9.2.8 Question 47

#### Our organization welcomes vulnerability disclosures by good-faith cybersecurity researchers

Discussions across aviation organizations and good-faith researchers have highlighted a wide variety of perspectives on how welcome vulnerability disclosures from external parties were in the aviation sector. This question asked respondents to give perspectives on whether their organization welcomed vulnerability disclosures by good-faith researchers.

#### 9.2.9 Question 48
#### Interactions between good-faith researchers and the aviation industry that I have been involved in were

Further exploring the interactions between good-faith researchers and the aviation industry, this question explored contributors' perspectives on these interactions.

## 9.3 INCIDENT MANAGEMENT

Irrespective of the effort put into preventing accidents or incidents, the aviation industry fully understands that they still occur. Years of hard-won experience and development of best practices have resulted in globally agreed-upon rules and regulations that ensure robust and objective investigation, with the objective of never suffering the same accident or incident twice.

There is a clear and well-understood process to deal with flight-safety incidents. But, with digitized and connected systems now underpinning operational safety, how to prepare for, identify, manage, and learn from aviation-cybersecurity incidents will be critical if the sector is to continue its hard-won track record on preventing incidents.

#### 9.3.1 Question 10
#### Preparation for aviation-cybersecurity incidents

This question explored perspectives on how well the respondents thought their organization was prepared for an aviation-cybersecurity incident.

#### 9.3.2 Question 34
#### Cybersecurity-awareness training

The need for good cybersecurity is well understood across many organizations; therefore, the need for awareness training is also well understood. This question explored cybersecurity-awareness training across all staff, and set up comparative perspectives for the next questions, which focused more on operational-security aspects.

#### 9.3.3 Question 33
#### We have an appropriate cybersecurity culture in place

For many years, the aviation industry has successfully woven a flight-safety culture into all flying operations. This has resulted in lower accident rates, and a culture in which all personnel consider flight safety a personal responsibility. With the recent ICAO Cybersecurity Strategy strongly encouraging the development of an aviation-cybersecurity culture, understanding and promoting this will be critical going forward. This question explored whether respondents thought their organization had an appropriate cybersecurity culture in place.

#### 9.3.4 Question 35
#### Our operational staff is trained to recognize a potential aviation-cybersecurity incident

Where the previous question looked across all staff, this question focused on whether operational staff is trained to recognize a potential aviation-cybersecurity incident.

#### 9.3.5 Question 36
#### Our operational staff is taught how to manage a potential aviation-cybersecurity incident

Recognition of a potential aviation-security incident is only the first step; this question explored whether operational staff was taught how to manage a potential aviation-security incident.

#### 9.3.6 Question 9
#### If a cybersecurity incident ever affected aircraft operations, the management of the incident would be led by

This question explored perspectives of the stakeholders and leadership when managing aviation-cybersecurity incidents.

#### 9.3.7 Question 29
#### Exercises

Across enterprise IT, security exercises ranging from small tabletop-exercises to large-scale, multi-organization exercises have proven their value. This question explored if contributor organizations conduct exercises replicating aviation-cybersecurity incidents.

#### 9.3.8 Question 15
#### Following an aviation accident or incident, any potential cybersecurity aspect is thoroughly investigated

Objective, rigorous investigation of aviation accidents and incidents has been a cornerstone of improving aviation safety and security for many years. With digitized and connected systems now underpinning the safety of flights and operations, this question explored if the potential cybersecurity aspects of accidents or incidents are thoroughly investigated.

#### 9.3.9 Question 14
#### Cybersecurity data availability and protection

To both discover and investigate any potential cybersecurity incident, access to cybersecurity-relevant data is critical. Capturing these data and protecting them from adversary interference will be as critical for the aviation sector as every other. This question explored if these data are captured, protected, and available for analysis.

#### 9.3.10
#### The role and challenge of cyber insurance
There is an increasing market for cyber insurance as companies incorporate it as an element of risk management. These two questions ask respondents if their organization includes cyber insurance as an element of managing their aviation cybersecurity risk. The next question explored their perspective on how easy they believed it may be for insurance underwriters to assess that risk.

#### 9.3.11 Questions 26 and 50
#### Communicating with external stakeholders on aviation cybersecurity and media organizations report aviation-cybersecurity issues in an informed and balanced manner
As part of normal business, and during any cybersecurity incident, effective and clear communication is essential to help manage and mitigate loss. For many stakeholders, aviation cybersecurity has been a challenging topic to discuss with external stakeholders. There is also a perceived nervousness about reporting on the topic of aviation cybersecurity.

These questions explored both how the respondents felt about communicating with external stakeholders and perspectives on how media organizations report aviation-cybersecurity issues. Respondents suggested that even aviation-industry media "have struggled to find enough best practice examples and so have generally not been able to write about the issue with any purpose."

## 9.4 REGULATIONS, STANDARDS, AND BEST PRACTICES
With the cybersecurity challenges facing the aviation industry, regulations, standards, and the development of best practices are, and will continue to be, an increasing cornerstone of systemically understanding and reducing risk globally. This section explored contributor perspectives across this important topic.

#### 9.4.1 Question 20
#### Current aviation-cybersecurity regulations are effective
Aviation-security regulations already exist, but this question sought perspectives on whether respondents thought they were effective.

#### 9.4.2 Question 21
#### Current aviation-cybersecurity regulations are clear and well understood
Following on from the previous question, this question explored whether the regulations in place were considered clear and well understood.

#### 9.4.3 Question 22
#### Current aviation-cybersecurity standards and best practices are well communicated
This question explored if the respondents believed the current standards and best practices are well communicated.

#### 9.4.4 Question 16
#### I feel well supported on aviation cybersecurity issues by industry bodies (such as IATA, CANSO, ACI, AAPA, etc.)
With the number and variety of aviation organizations, it is no surprise that many have aligned themselves with an industry body that represents their interests. Many of these bodies do more than just represent their members' interests, and are also starting to provide support on aviation-cybersecurity topics. This question explores that support.

#### 9.4.5 Questions 17, 18, and 19
#### Support from standards and rulemaking bodies (such as ICAO, EASA, etc.) and where aviation-cybersecurity regulation should be led from.
With the increased focus on aviation security, support from standards- and rule-making bodies will be essential to help organizations quickly understand and manage risk. This question explored perspectives around that support, and where contributors thought aviation-cybersecurity regulation should lead.

#### 9.4.6 Questions 23, 27, and 28
#### Advice on best practices, and guidance and satisfaction on accessing that guidance
With a multitude of stakeholders, organizations, and operations, understanding where people look for advice on aviation-cybersecurity best practices and guidance will be helpful when looking to develop and disseminate best practices. The following question explored contributor satisfaction with their ability to access that advice, including from their states.

#### 9.4.7 Question 18
#### My organization is planning on investing more in aviation cybersecurity
Is this a potential growth area for spending?

# About the Authors

**Pete Cooper** is CEO of Pavisade, advising on cyber strategy across multiple sectors including aviation. Prior to the commercial sector, Pete was a Royal Air Force fast jet pilot, then moving into the cyber domain as one of the first military operations officers before becoming the first Strategic Cyber Operations adviser to the UK Ministry of Defence (MOD). Pete holds a Post Grad in Cyberspace Operations and has published on the topic of developing legal active cyber defense strategies to disrupt advanced cyber threat actors.

He is a trusted adviser on aviation cybersecurity at international, national and organizational levels. He was the author of 'Finding Lift, Minimizing Drag', which explored the cybersecurity challenges facing the global aviation sector and advised how regulation, policy and strategy should be developed nationally and internationally to counter the next generation of threats and adversaries. Additionally, he is the lead of the Aviation Village at DEF CON, the world's largest hacker conference, with the aim being to build trusted relationships between the research / hacker communities and the aviation sector. This means he works closely with organizations such as US Department of Homeland Security, the US Air Force, international aviation bodies and the aviation industry.

He is also a Fellow of the Royal Aeronautical Society, Atlantic Council Cyber Statecraft Senior Fellow and the founder and Director of the UK's only student cyber strategy challenge, designed to develop and highlight the next generation of cybersecurity leadership. Additionally, in 2018 he was judged 12th on a list of global cyber security influencers by IFSEC.

**Simon Handler** is a program assistant with the Atlantic Council's Cyber Statecraft Initiative, within the Scowcroft Center for Strategy and Security. In this role he manages a wide range of projects at the nexus of geopolitics and national security with cyberspace. Prior to joining the Atlantic Council, he served as a special assistant in the United States Senate. Simon holds a BA in International Relations & Global Studies, with a concentration in International Security, and Middle Eastern Languages & Cultures from the University of Texas at Austin. He serves as a Board Director and Community Service Chair of the Texas Exes of Washington, DC. He speaks Arabic.

**Safa Shahwan** is the assistant director of the Atlantic Council's Cyber Statecraft Initiative within the Scowcroft Center for Strategy and Security. In this role, she manages the administration and external communications of the Initiative, as well as the Cyber 9/12 Strategy Challenge, the Initiative's global cyber policy and strategy competition. Safa holds an MA in International Affairs with a concentration in Conflict Resolution from the George Washington University Elliott School of International Affairs and a BA in Political Science from Miami University of Ohio. Safa is of Bolivian and Jordanian heritage and speaks Spanish and Arabic.

# Acknowledgments

First, a huge thanks to a great number of participants and contributors throughout this report. This includes those who participated in the survey, helped distribute it, and took part in the workshops, additional interviews, and conversations.

Second, thank you to Thales for underwriting and supporting this global survey and report. Its commitment to safety and collaboration across stakeholders in this diverse industry is evident.

And third, to the members of the Atlantic Council's Cyber Statecraft Initiative, within the Scowcroft Center for Strategy and Security. In particular, special thanks are due to Meaghan Byrne, Simon Handler, Trey Herr, and Safa Shahwan for their assistance and coordination of this project.

The report objective was to explore a considerably complex topic discussed in both open and closed forums. Therefore, omissions of content or errors contained within the paper are the author's own responsibility, and not a reflection of the on- and off-the-record contributors whose candor and time helped make this paper what it is.

# Atlantic Council Board of Directors

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.



Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org