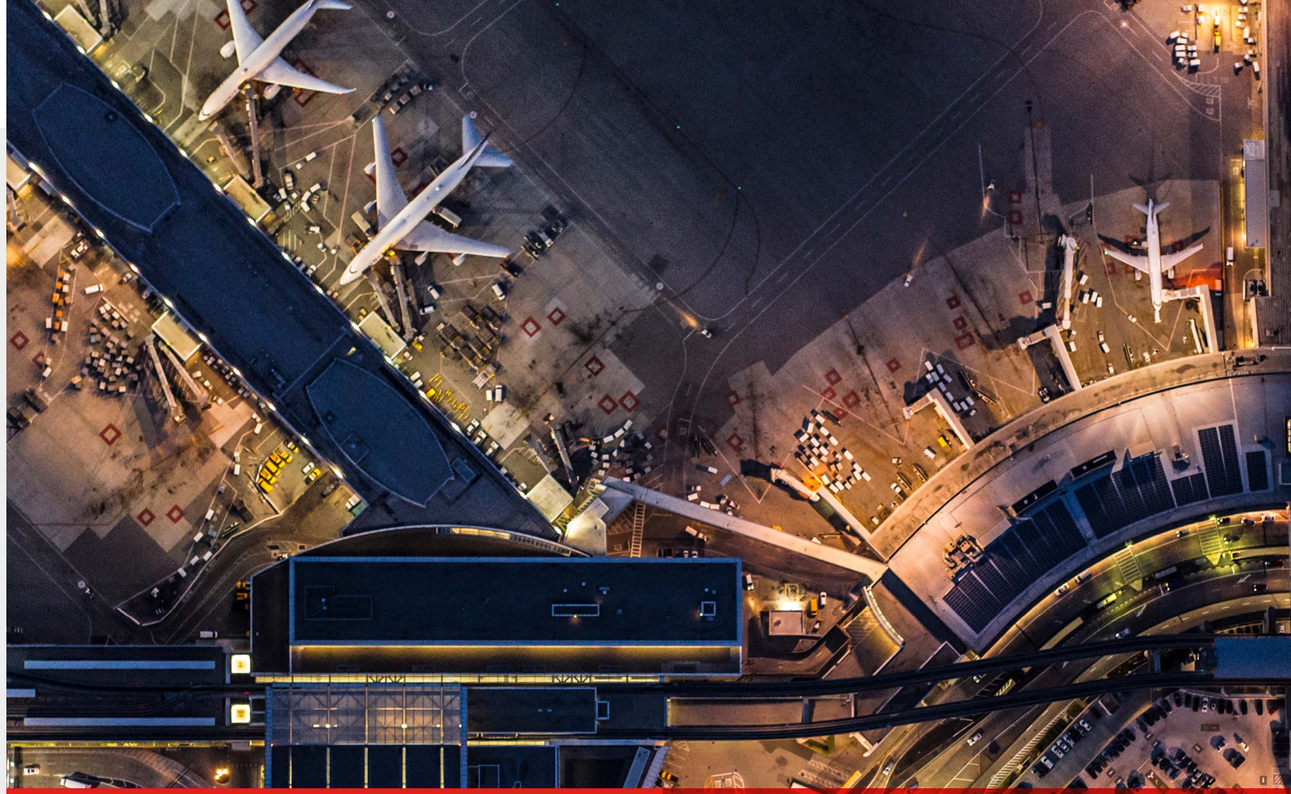
Aerospace Agenda: Cybersecurity

Ensuring safety, cyber resilience, and digital trust in the aerospace industry



A BSI insights paper

Executive summary

Until early 2020, the aerospace sector was building towards unprecedented growth. However, the COVID-19 pandemic has had industry-changing impacts on the global aerospace economy, bringing seismic changes to the sector; its ways of working and its ecosystem. Aligned to the success of global COVID vaccination programs, the aerospace sector is now charting a path to recovery.

Whilst passenger planes were grounded, technology advances in business took off at an exponential pace. The COVID-19 pandemic has accelerated digital working by five years (McKinsey 2020), and whilst technology has continued to progress, the risk posed by information and cybersecurity threats has also accelerated.

Safety and security have always been of paramount importance for aerospace, and the sector has built a good reputation in these areas. However, with the continuing growth, pace and complexity of digitization, comes the potential for significant cybersecurity risks, increasing the likelihood of cybercrime and the inevitability of critical safety and cybersecurity breaches. Examples from within the aerospace sector include loss of passenger data and intellectual property theft, presenting commercial, reputational, and security challenges.

Exponential growth in data volume across the industry, accompanied by the need for users to access multiple systems remotely and the increasingly interconnected nature of aerospace technology, across airframes, airside operations, landside operations and ultimately passenger interfaces have dramatically increased the “attack surface,” both in the air and on the ground.

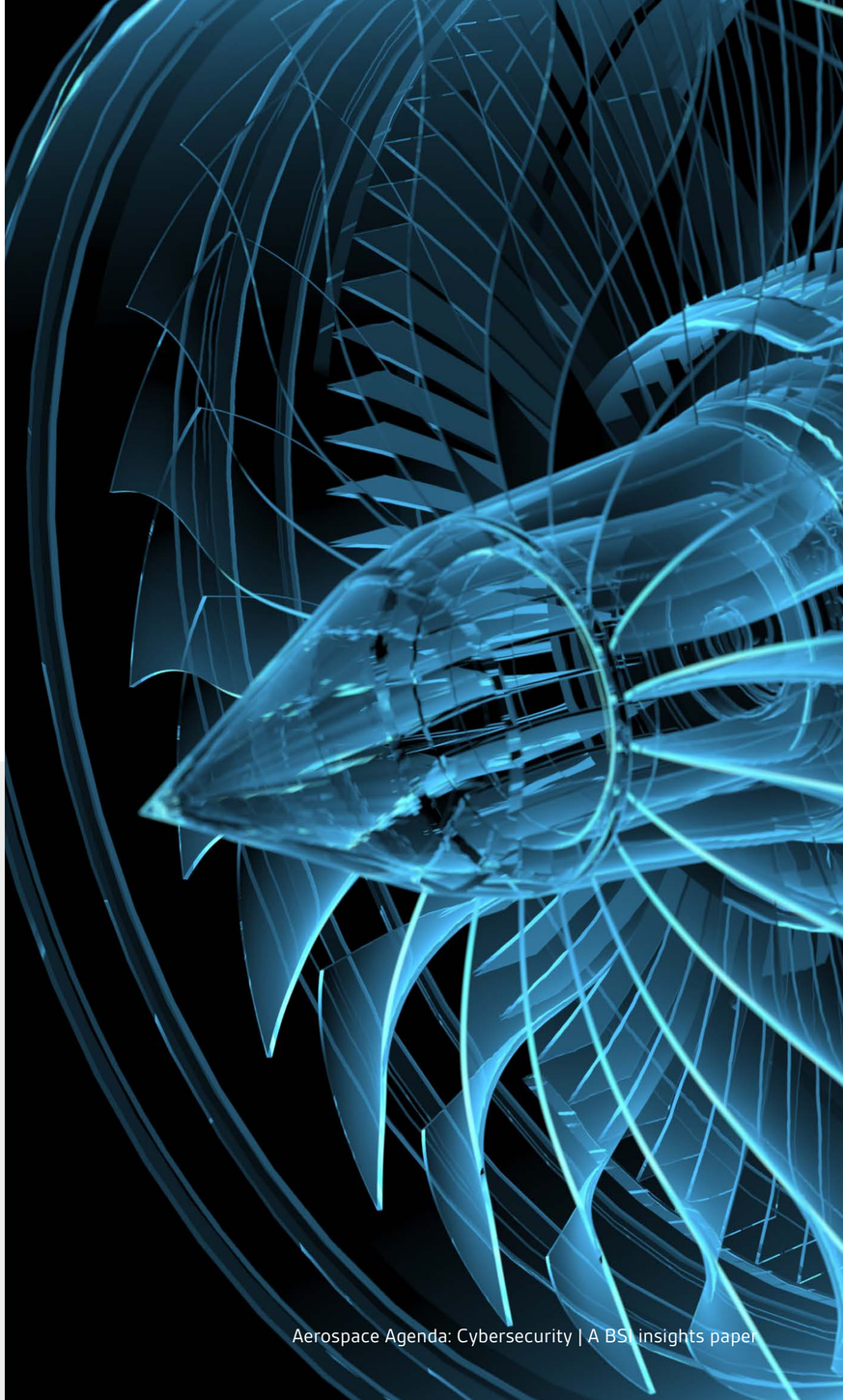
Regulation is challenged by the sheer speed of change, and regulation therefore can actually delay the adoption of new technology, creating opportunities for unauthorized cyber actors, including criminals and terrorists. The absence of advanced regulation or conformity standards can also create exposure to malaise and over-confidence in the use of new technologies which can have disastrous consequences at time of failure, if not rigorously tested and validated in simulated operations.

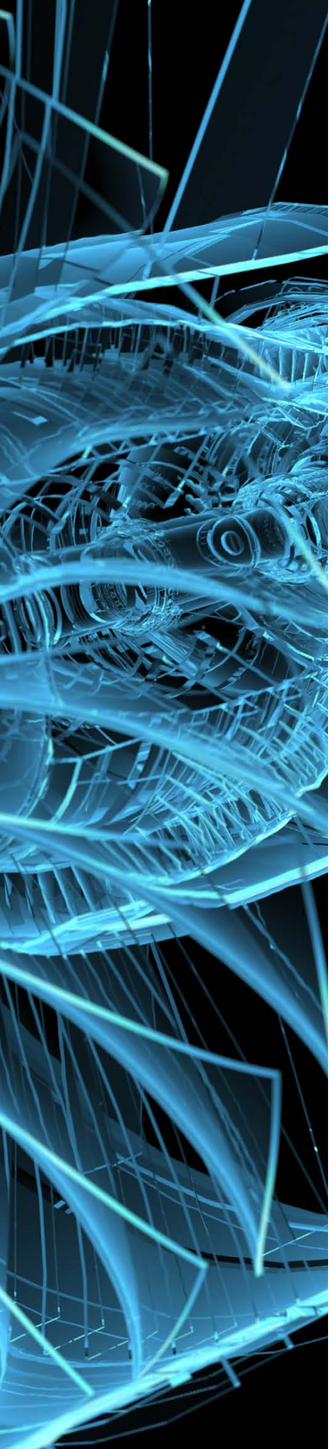
Industry stakeholders, including airlines, aircraft manufacturers and suppliers, airport operators, air traffic controllers and border authorities, need to act to counter information and cybersecurity risks and build in safety, digital resilience and trust.

They have a responsibility to safeguard people, protect physical infrastructure, ensure regulatory compliance, build brand reputation and ensure continuing confidence in the travelling public of the security of their personal data as individuals, as well as the airworthiness of the ever-advanced technology being used in aviation. The challenges faced by the defence sector are similar.

The key to cyber resilience is to embed the aerospace sector’s strong culture of commitment to safety into its response to maturing cybersecurity risk management. Aerospace organizations will need to adapt their mindset: in today’s digital world, cyber-attacks will come from multiple sources and with increasing persistence, so the industry’s response should be to demand equally dynamic solutions, and recognize the need to deploy mitigation against such cyber-risks both externally and internally.

Now is the time for aerospace organizations to respond to the cybersecurity challenge.





Contents

Introduction

The global COVID-19 pandemic hit few industries as hard as the commercial travel and aviation sector, with aerospace closing down overnight in many countries. Passenger planes were grounded as many countries went through a series of lockdowns, and when they did fly, it was at greatly reduced capacity. According to a recent McKinsey report, airline revenue in 2020 was down by 40%, to the levels seen in the year 2000.

Before COVID-19, the aerospace sector was experiencing huge growth and development. The International Air Traffic Association (IATA) had expected passenger numbers to reach $7.2 billion by 2035, and experts had projected a rapid increase in commercial aircraft production, from approximately 1,500 aircraft in 2018 to 2,200 per annum by 2035.

It is anticipated that the aviation sector recovery will be slow and fuelled primarily by leisure travel rather than the more lucrative business travel. To reduce operating costs, many in the commercial aerospace industry will increasingly rely on digital solutions to maximize their impact, streamline their operations and provide new, immersive and client-interactive digital services to improve the customer experience.

While an increased reliance on information systems, implementation of Artificial Intelligence (AI) and connected devices will maximize efficiencies, this digital transformation could simultaneously increase the sector's cybersecurity vulnerabilities.

And, across the wider sector, the increase in remote or homeworking has further contributed to greater information and cybersecurity risks for aerospace organizations.

Safety and security

From the inception of commercial air travel, flight safety and security have always been of paramount importance to the industry, which has historically had a good security record and reputation. While air accidents and safety incidents capture headlines and fuel passenger anxiety, research shows that flying remains a remarkably safe way to travel when compared to road and rail.

But aerospace leaders could be forgiven for still feeling anxious. Barely a day goes by without the publication of another report on the increasing scale and complexity of cybersecurity risks, or the emergence of yet another cyber threat, challenging industry leaders as they recognize the need to embrace innovation to advance the aerospace sector.

In general, the number of cybersecurity breaches are high and increasing. They are becoming more sophisticated, and their impact more damaging. Although the stigma associated with a cyber-breach is reducing, they are becoming more commonplace. The global 'State of Cybersecurity 2020 Report' from the cybersecurity industry body, Information Systems Audit and Control Association (ISACA), indicates that 32% of organizations responding to ISACA's annual survey are experiencing an increase in cyber-attacks.

The National Cyber Security Centre (NCSC), the UK's top cyber-defence centre, says it has stopped Britain falling victim to almost 1,200 attacks in the last two years – about 10 attacks every week. With at least 63 countries having cyber-attack capability, it believes state-sponsored hackers employed by hostile nations carried out most of the attacks. In 2021 Irish Health IT services were shut down following a ransomware attack, and in the US the Colonial Pipeline hack cut off a large portion of the East Coast's fuel supply.

Digital transformation

The rapid integration of universal digitization provides the backdrop to the growing cybersecurity threat. The aerospace sector has embraced an ongoing process of digital transformation, using technology to improve user experience and enhance commercial performance.

Travellers have been enjoying an increasingly efficient 'end to end' customer experience in recent years, thanks to digitization. Airport operations have become smarter and safer, improving self-service and passenger engagement. This has resulted in the emergence of new non-core revenue streams (shopping, entertainment etc.) and new business models.

The trend for digitization has accelerated yet further due to the COVID-19 pandemic, with increased reliance on the digitization of the safety, security, hygiene and immigration phases of the passenger experience; from booking and pre-travel checks, to movement through the departure airport and onward to the destination airport.

On board the aircraft, passenger experience has been transformed by in-flight connectivity. Indeed access to the internet could be a factor in winning back business travellers, by enabling the aircraft to become an extended office. Recent research from FlightGlobal finds eight out of 10 passengers fly with their own wireless device, with most using it to connect to in-flight internet. The study puts the value of in-flight connectivity – through Wi-Fi, wireless entertainment, live TV, mobile voice and texting – at US$4 billion. Another study, from satellite operator Inmarsat, finds that half of passengers would choose Wi-Fi availability over inflight meals or alcoholic drinks. This increased adoption is fuelling the transition towards hyper-connectivity.

Hyper-connectivity

The quest to complete tasks faster and more efficiently has resulted in the increasing interconnection of systems. Airlines, airports, aviation authorities, air traffic management, aircraft manufacturers, and the supply chain (maintenance, catering etc.) are becoming increasingly dependent on each other's systems and data. System connectivity is exemplified by the evolution of the Airport Collaborative Decision Making (A-CDM) concept. Airports implementing A-CDM act as data intermediaries and a single source of truth for stakeholders as diverse as airlines, ground handlers and even passengers.

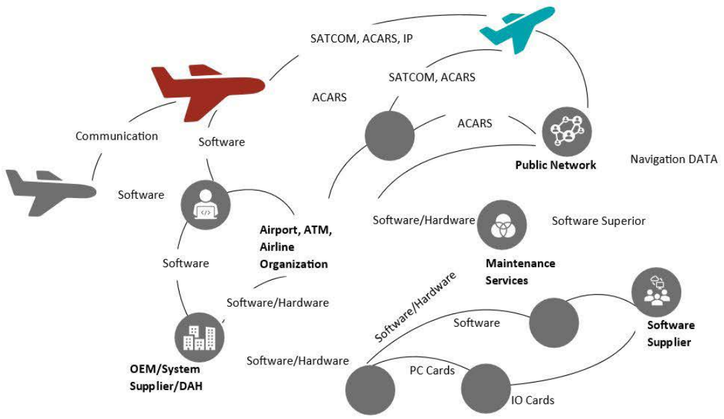
Digital transformation

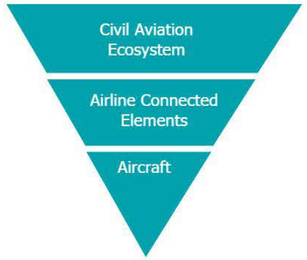
Rising data volumes

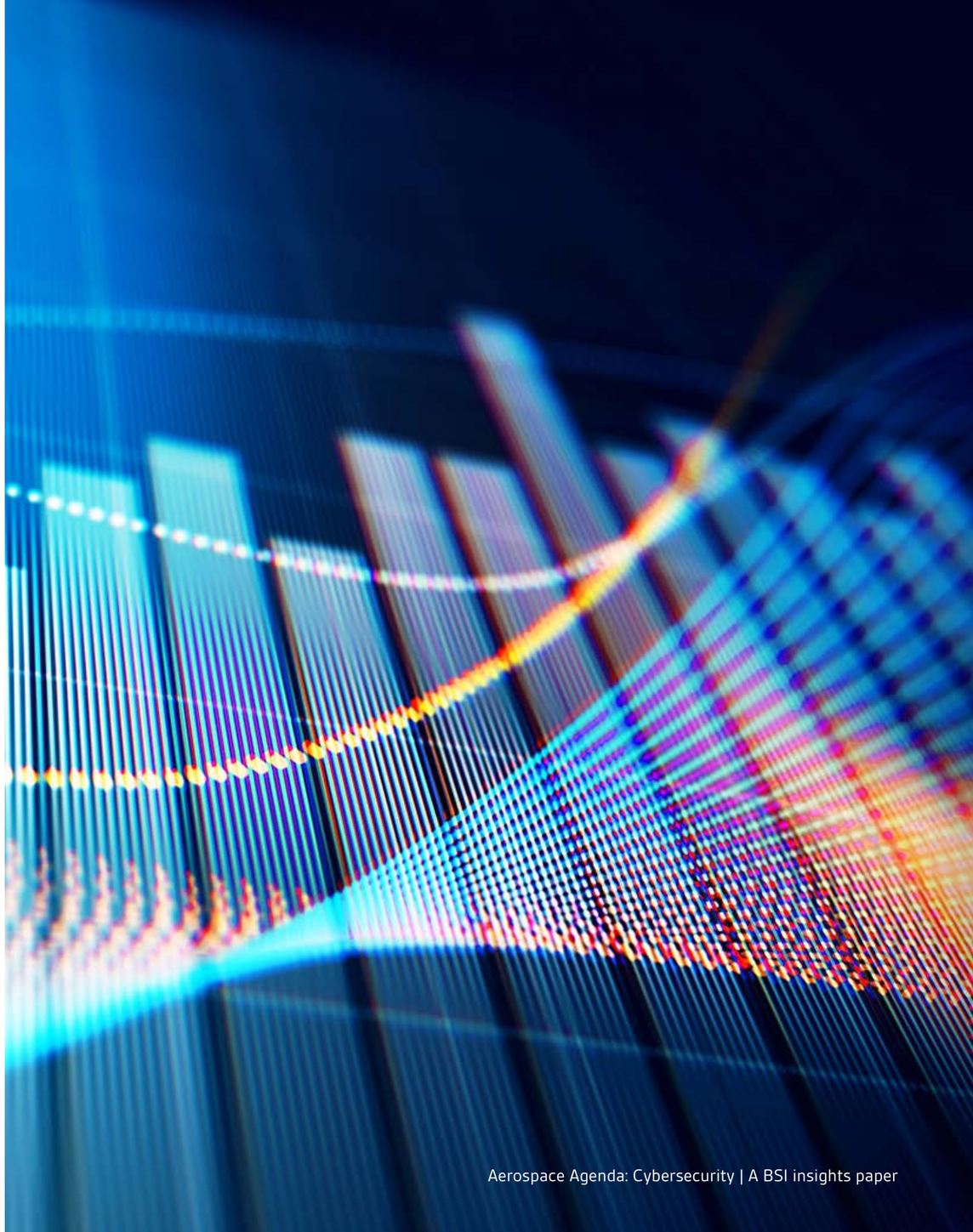
It's clear to see the critical role data plays in propelling the industry forward and re-shaping the sector as a whole. Sound business strategies require data-driven insights to support decision-making and innovation.

With the increasing deployment of digital technology and connectivity has come an exponential growth in data. For example, it is estimated that by 2026 aircraft systems will generate a massive 98 million terabytes of data – driven by everything from pilot decision support (such as dynamic weather and route optimization data), to passenger experience, retail and entertainment (in-flight access to Amazon, Netflix, Spotify, YouTube etc.).

Another huge demand on data comes from the need to improve maintenance efficiency through real-time monitoring. The more accessible the data – especially remotely – the more expediently and easily aircraft can be maintained, with reduced downtime.







The cybersecurity risk landscape

Rising connectivity and data volumes create significant opportunities – in terms of new revenue streams and cost efficiencies for airlines and their supply chain partners. But they also bring more cybersecurity risk. Increasing dependence on data and connected systems is enlarging the potential 'attack surface' – that is, exposing additional potential weaknesses to cyber-attack.

Industry-wide standardized networks create further systemic risk, while sharing of intellectual property, such as designs, research and cutting-edge technology, raises the stakes still higher. By sharing the same non-proprietary technology, aerospace industry systems are becoming more interoperable and therefore more efficient to maintain – for example, by training technicians in the same skills throughout the supply chain. But if vulnerabilities are found in a technology, all the systems depending on it will be affected. Furthermore, the wider adoption is leading to more people becoming skilled in using the standardized technology, and therefore making these skills more accessible to threat actors.

Take aircraft communications: with more advanced chipsets come more sophisticated aircraft networks, moving from low bandwidth, point-to-point proprietary communications to high bandwidth, ubiquitous TCP/IP-based digital systems. On the ground, migration from legacy radar systems and beacons to digital communications (ADS-B) provides improved accuracy and reliability, but with these technological advances come new and often increased risks, for example, is ADS-B effectively encrypted? If not, it could allow electronic eavesdropping with low-cost equipment, open source software and widely known techniques. The example highlights that the aerospace industry needs to consider the cybersecurity risks associated with switching from old systems to new technologies, including back-ups.

1. Volatility in geographic and economic environment
2. Managing the supply chain
3. Competition in domestic and international markets
4. Managing and retaining talent
5. Ability to perform on key contracts
6. Compliance with a wide range of regulations and restrictions
7. Capacity to innovate
8. Failure to realize the benefits of M&A and partnerships
9. Exposure to cyber security events
10. Foreign currency and commodity price fluctuations

The cybersecurity risk landscape

Cybersecurity risks in the air

Hackers can potentially exploit security holes to spoof flight information such as map routes, speed statistics and altitude values, and steal passengers' credit card information. In extreme circumstances, illicit actors could take control of entire aeroplanes under cyber-hijack or to establish the ultimate timebound ransomware threat.

While developers of newer In-Flight Entertainment (IFE) systems have incorporated additional security features into their engineering, many IFE systems currently in use can be as much as 10 years old with little, if any, security upgrades.

In addition, the increased use of "electronic flight bags" (EFB) and electronic manifests, along with multiple options for passenger credit card purchases, including microservices payments through loyalty schemes, all dramatically increase cybersecurity challenges. Regular software updates to on-board systems may go some way to addressing the challenges.

Cybersecurity risks on the ground

May 2018 saw the introduction of the General Data Protection Regulation (GDPR) across the EU, imposing one of the world's most comprehensive and heavily enforced data breach notification regimes.

Under the GDPR, organizations in the EU can be fined up to 4% of global annual turnover for data breaches. In July 2019 a major airline was fined a record £183m from the Information Commissioner's Office (ICO) for a breach of its security systems in 2018. It was the largest penalty imposed by the ICO and the first to be made public under the GDPR.

Hackers had carried out a sophisticated, malicious criminal attack on the airline's website. The incident took place after users of the website were diverted to a fraudulent site, where the cyber criminals harvested details of 500,000 customers. Names, email addresses and credit card details, including card numbers, expiry dates and three-digit CVV codes were stolen.

Cybersecurity experts believe a hacker managed to get a script onto the website and app, so that as customers typed in their credit card details, a piece of malicious code was able to extract this information illicitly. Known as a 'supply-chain attack', this is a growing threat to websites that embed code from third-party suppliers.

Commenting on the case, the UK's Information Commissioner, Elizabeth Denham said: "The law is clear – when you are entrusted with personal data, you must look after it. Those that don't will face scrutiny from my office to check they have taken appropriate steps to protect fundamental privacy rights."

Cybersecurity risks in the supply chain

US, European and Australian aerospace defence contractors have all suffered cyber-attack and loss of sensitive data and intellectual property to hostile foreign cyber actors.

In 2016, aviation expert Su Bin was sentenced to 46 months in jail after admitting his role in stealing information on key military aircraft, having successfully hacked the networks of US and European defence contractors.

Separately, in Australia in 2016, a cyber attacker nicknamed 'Alf' gained access to a defence contractor's computers, enabling him to snare data on sophisticated US weapons systems. Using simple combinations of login names and passwords and exploiting a vulnerability in the company's helpdesk portal, 'Alf' roved the firm's network for four months, obtaining data on Australia's planned purchase of fighters and maritime-surveillance aircraft.

These examples highlight the need for increased trust within the supply chain, and the ability to establish and verify how suppliers use and control data throughout the lifecycle.

In search of resilience

Technology is moving faster than regulation can react, creating inconsistencies in the application of security measures and standards across the aerospace industry – and creating opportunities for unauthorized cyber actors.

Experts agree that systems should be designed with the assumption that they will be compromised at some point. As in the physical world, even with the doors locked and alarms fitted, break-ins can occur. Sooner or later businesses – or their suppliers – will have a breach from their 'soup' of systems, their processes, or their people. One of our recent research studies shows that 39% of European organizations have experienced a data breach in the last 12 months – yet one-in-six currently remain unprepared for a breach.

Airlines, aircraft manufacturers, airport operators and other industry stakeholders need to act to counter the risks. They are responsible for protecting infrastructure, ensuring regulatory compliance and safeguarding people. Controls include establishing the right governance framework at board level, ensuring technical measures on secure configuration, network security, malware prevention and mobile working, and addressing 'people' issues such as user privileges, education and awareness, and measures to prevent potential bribery or blackmail of staff.

The industry also needs to adapt its mindset. While 20 years ago the accepted approach to cybersecurity was to detect weaknesses and prevent breaches by constructing technological 'walls', such defences will not neutralize today's threats. Cyber-attacks are multiple and constant – and not restricted to the perimeter of corporate networks.

The challenge now is to identify and respond to threats and improve defences constantly – solutions must be dynamic – in the air (flight control systems etc.) and on the ground (hardware provenance, supply chain risk). For example, the NCSC's Active Cyber Defence programme, uses a mix of automated processes to defeat internet-based threats to the UK. One focus is to take down malware and phishing sites, with 64% of illegal sites offline within 24 hours of being discovered.

Given the dynamic nature of the risk, aerospace boards are advised to review threats and vulnerabilities on a regular basis, ensuring their investments to control cyber threats are effective. They also need to develop the skills and capability to understand how the risk could affect them and what strategic response is required. With an assumption of future breach, emphasis must be on resilience and 'breach management' – in effect, building the capability to withstand a breach and continue 'business as usual'.

Preparation is vital. Implementation of best practice, internationally-recognized standards, awareness training and ongoing testing are crucial. BSI's recent research has found that, while 73% of organizations say they are concerned about cybersecurity and seeking solutions, one-in-six highlighted that they had no plan in place. When asked if their organization was undertaking cybersecurity testing, over a third stated that they were not.

Help is at hand

From standards to product and system certification, training, consulting, and software solutions*, BSI works with a broad range of primes and suppliers across the commercial, defence and space manufacturing supply chains, as well as the full aviation sector vertical, including airlines, airports and ground handlers, to address the sector's challenges, raise standards, meet compliance requirements, embed resilience and drive innovation.

Management System Certification and Standards

Standards are a tried and tested way to work more efficiently and effectively. They help organizations to improve their performance, reduce their risk and help them be more sustainable.

ISO/IEC 27001 Information Security Management

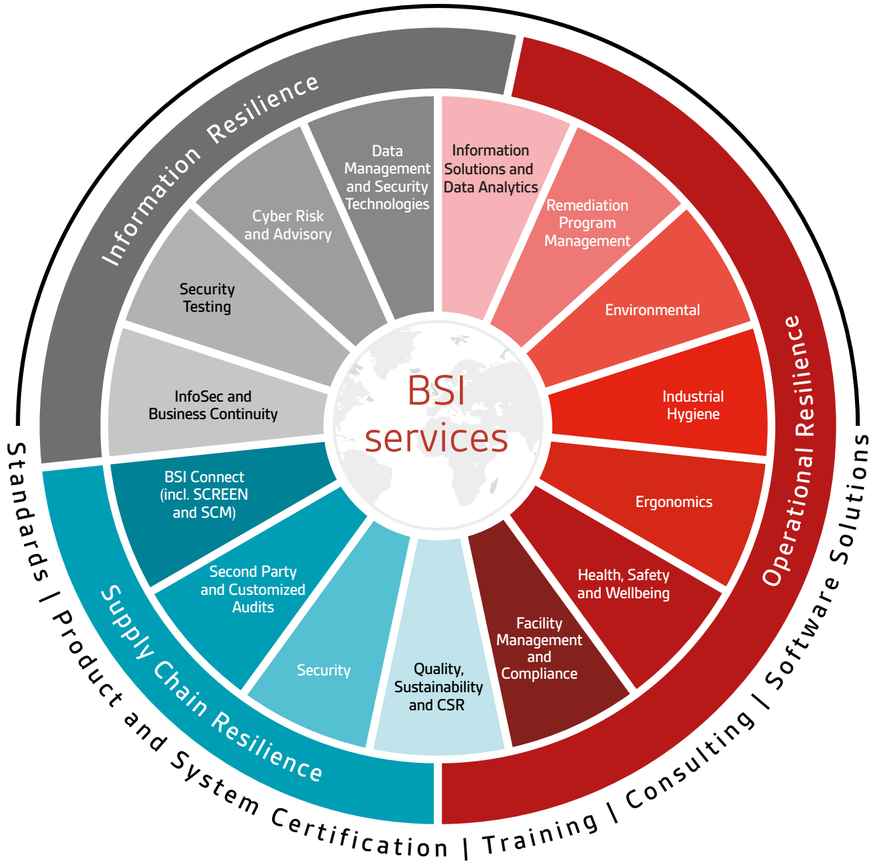
Organizations which adopt ISO/IEC 27001 create a process-based approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System (ISMS). It can be used in conjunction with AS/EN 9100 and ISO 22301 to assure information resilience and business continuity and develop greater organizational resilience, should the confidentiality, integrity or availability of information be compromised. All three standards are technology agnostic and applicable to aerospace organizations of any size. BSI certification to ISO/IEC 27001 helps aerospace organizations to:

- Demonstrate to their internal and external stakeholders their commitment to effectively managing information security
- Reduce the risk of a breach of confidentiality, non-availability, or loss of integrity of business-critical information
- Reduce the likelihood of staff-related information security breaches through heightened staff awareness of risks
- Minimize the business impact and cost of incidents and disruptions
- Reinforce brand reputation and stakeholder confidence through public affirmation of commitment to information security
- Build trust in the marketplace, helping to win more business through a demonstrable "security licence to operate"
- Simplify the process of achieving compliance with relevant legislation and reduce the likelihood of prosecution and penalties
- Strengthen organizational resilience

ISO 28000 Supply Chain Security Management

The global transportation of goods has never been so complex., It poses many threats for organizations including theft, terrorism, smuggling, preservation of brand integrity and product safety. However, organizations can demonstrate that they have identified critical aspects to the security of their supply chain and have policies, procedures and controls in place to manage security risks with ISO 28000 from BSI.

ISO 28000 brings big benefits to companies of all sizes. By allowing you to respond to the increasing customer demands for proof of systematic security management, an ISO 28000 compliant management system can improve your business confidence, reputation and future growth.



*BSI Group recognizes and respects the need to maintain impartiality through separation of BSI's Assurance Services, Regulatory Services and BSI Consultancy Services. As such, BSI cannot offer management systems consultancy and certification services for the same scope to the same organization.

Cybersecurity and Information Resilience Consulting

Information Resilience, a domain of Organizational Resilience, empowers organizations to safeguard their information – physical, digital, and intellectual property – throughout its lifecycle, from source to destruction. This requires the adoption of information security-minded practices that enable stakeholders to gather, store, access, and use information securely and effectively.

Cybersecurity and Information Resilience (CSIR) at BSI gathers a global team of expert consultants that help organizations to:

- Better respond to cyber threats and build more resilience around their critical information and IT infrastructure
- Protect their information, people, and reputation
- Enable a state of enhanced and sustainable information resilience through

Our services help organizations achieve a state of enhanced and sustainable information resilience through our integrated and woven sets of products and services.

Cybersecurity

This ranges across a broad spectrum of testing and vulnerability management services, from penetration testing to gold standard Red Teaming (CREST approved). BSI's expert Attack Simulation also includes Physical Security, Blue Team, and Purple Team to provide a broad scope with a holistic view of the organization across multiple information security domains.

Within these services, BSI also provides a host of cloud security solutions, from web security and application testing, to social engineering, identity access management and data protection in the cloud.

Information management and privacy

With the proliferation of global legislation including the GDPR and CCPA, privacy management and data protection has never been under so much scrutiny. Organizations need to be compliant, transparent, open, and fair in what they do with personally identifiable information (PII).

Organizations need to have controls in place for how they acquire information (do they have consent?), use data (do they have permission?), and archive and destroy data (the right to be forgotten and erasure. When an organization suffers a breach, BSI provides forensic capability to identify where the breach occurred and if the data was compromised.

Security awareness and training

BSI implements robust, agile, and compliant training modules and courses to ensure that your weakest link becomes your strongest asset in remaining vigilant and resilient to the omnipresent threats.

Additionally, BSI offers bespoke, customized, online, in-house, and classroom-based certified training courses across a mix of information security, cloud security, and data protection courses.

Compliance to requirements

With support for PCI DSS to NIST framework, Cyber Lab certification to ISO 27001/27701 implementation, and HIPAA to SOC 2 services, BSI enables organizations to ensure compliance through our knowledge of the standards and regulatory landscape and our highly experienced teams of consultants.

*BSI Group recognizes and respects the need to maintain impartiality through separation of BSI's Assurance Services, Regulatory Services and BSI Consultancy Services. As such, BSI cannot offer management systems consultancy and certification services for the same scope to the same organization.

Looking ahead

The key to safety, resilience and trust is to embed aviation's longstanding strong safety culture into the relatively young, maturing industry of cybersecurity risk management. There is a lot that the two disciplines can learn from each other, so they must work together to meet today's cybersecurity threat.

Specific developments in aerospace sector niches also have much to offer this global industry. For example, the US Department of Defense's Cybersecurity Maturity Model Certification (CMMC) sets cyber standards and practices to help the US defence industry reduce exfiltration of controlled unclassified information. Created in cooperation with the Aerospace Industries Association and other stakeholders, the CMMC model should be widely adopted, with five levels ranging from basic cyber hygiene to highly advanced practices.

BSI understands today's cybersecurity environment and the challenges it poses to the aerospace industry. We have the expertise to help aerospace leaders gain confidence to make sense of the changing industry risks and put robust measures in place to manage and mitigate them.

Whether it is the assurance provided through training and certification to key management system standards, including AS/EN 9100, ISO/IEC 27001 and ISO 22301, or more specific cybersecurity risk management support services, from security awareness training to penetration testing, our teams can support organizations in creating safety, resilience and trust.

About the authors

Brendon Hill,

Global Head of Aerospace, BSI

With over 40 years' experience in aerospace and engineering Brendon leads the strategic direction of BSI's aerospace sector. Brendon collaborates with industry bodies to drive innovation and is an international speaker, leading the way for a safe, secure future for the sector. Previous experience includes 26 years as a British Army Officer and Aircraft Engineer, both writing and implementing the quality management system and providing technical support to British Army aviation. He has worked at a senior level in manufacturing in aerospace and other high-risk sectors.

Brendon supports global organizations by helping them to understand and implement the concept of organizational resilience in every aspect of their business. Building business assurance into their strategy, aligned to the expectations of their clients and indirect customers, regulators and stakeholders.

Mark Brown

Global Managing Director, Cybersecurity and Information Resilience, BSI

Mark is an internationally recognized thought leader in Cybersecurity and Information Resilience and has held a number of global international leadership roles across multiple sectors, including Fortune 500 CIO, CTO and CISO roles. With almost 30 years' industry experience, Mark brings a wealth of practical industry and professional services knowledge including extensive proficiency on the Internet of Things (IoT) and the expanding cybersecurity marketplace as organizations grapple with digital transformation and addressing new technology that brings new business risks. In his role at BSI, Mark is responsible for driving BSI's global cybersecurity and information resilience strategy including a focus on expanding current services and bringing a new global focus on emerging technologies and risks such as IoT and Operational Technology (OT), increased cloud adoption, RPA Security, 5G security, and the CISO desire to achieve central management over the new converged digital arena, positioning cybersecurity as a true business enabler.

For more information on BSI's suite of cybersecurity solutions
Visit: bsigroup.com
Call: +44 345 080 9000

Why BSI?

From standards to product and system certification, training, consulting, and software solutions*, BSI works with a broad range of primes and suppliers across the commercial, defence and space manufacturing supply chains, as well as the full aviation sector vertical, including airlines, airports and ground handlers, to address the sector challenges, raise standards, meet compliance requirements, embed resilience and drive innovation.

*BSI Group recognizes and respects the need to maintain impartiality through separation of BSI's Assurance Services, Regulatory Services and BSI Consultancy Services. As such, BSI cannot offer management systems consultancy and certification services for the same scope to the same organization.