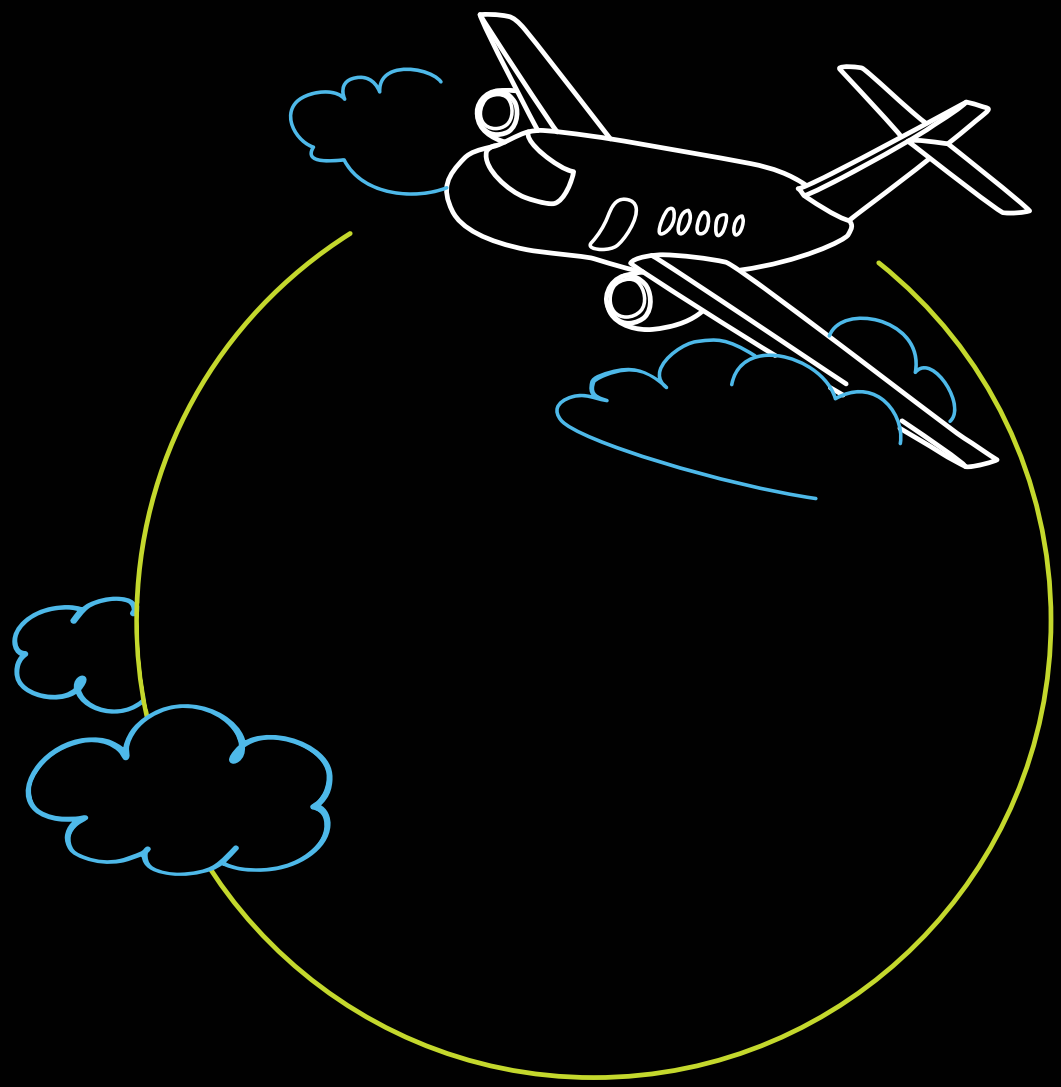
Deloitte.



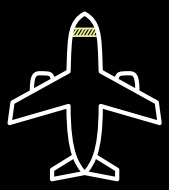
Please Fasten Your Seat Belts:
Managing digital risk to support aviation innovation

The typical discussion of cyber attacks usually revolves around stolen credit card data, breaches of personal information and identity theft. However, an increasing number of organisations have been hit with cyber attacks that extend well beyond the typical breach of employee or customer data. This new breed of cyber attack can target intellectual property, strategic plans and information about high profile people – or can be intended to cause operational chaos, destruction of corporate assets, or significantly threaten public infrastructure and safety. These are not traditional 'hackers' or cyber criminals. They can be nation-state actors or groups with a competitive, political or ideological agenda. While perhaps not considered acts of full-blown cyber terrorism, the latest cyber attacks are arguably entering the realm of cyber terrorism and cyber warfare in their scope and potential impact.

Cyber-risk is clearly no longer just about securing corporate data and maintaining data confidentiality, integrity and availability. Cyber-risk is an organisational risk, even an existential one to some organisations and can no longer be relegated solely to the domain of information technology (IT) to address. Cyber incidents can disrupt day-to-day operations, impose irreparable reputation damage and for the aviation industry, even threaten lives. Corporate boards around the country are asking: Is my organisation going to be targeted? For aviation companies – in the business of transporting millions of people safely with 100 000 daily flights at 11 277 meters – the stakes are especially high.

The innovation link

The aviation industry contributes 2.1% to the South African Gross Domestic Product (GDP), which is about R51 billion a year, a study commissioned by the International Air Transport Association (IATA). Another report done by Oxford Economics, a think tank, looked at the impact of aviation on countries' economies and found that aviation provides livelihoods for 227 000 South Africans. The average aviation employee generates R21 000 in gross value added - making them more than four times as productive as the average South African job. The study looked at 54 countries. Tony Tyler, IATA's Director General and CEO, attended the AGM of the Airlines Association of South Africa where the report was unveiled. Tyler said the report found that tourism enabled by aviation generates a further R21bn in economic activity and 116 000 jobs in South Africa.[1]



Growth rate of civil aviation
In 2015 aviation accounted for **2.1%** of the country's Gross Domestic Product (GDP)

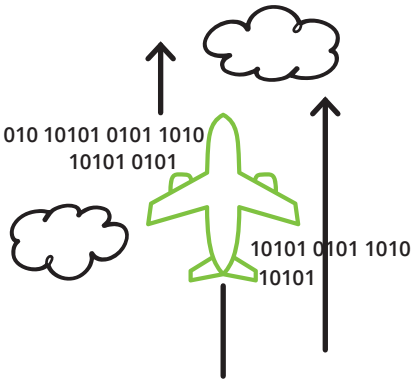
Economic activity
In 2015 aviation contributed **R51 billion** in total economic activity

Job creation
In 2015 aviation supported **227 000** jobs

[1] http://www.tomsa.co.za/index.php?nav=news&view=109

Rise of the digital aircraft

The new generation of aircraft is IP-enabled, also referred to as "e-enabled" or digital aircraft. These are the "smart devices" of the aviation industry, which are radically changing the way airlines operate from the flight deck, to the cabin and on the ground. These new innovations, some driven by aircraft technology, others by the handheld digital age, allow the industry to address longstanding operational inefficiencies to optimise fuel consumption, advance maintenance efficiency, improve scheduling and increase access to real-time quality data through capabilities such as GateLink (PKI), Electronic Flight Bags (EFB), Secure Aircraft Communications Addressing and Reporting System (ACARS)[2] and next generation air traffic control. The benefits of these technology innovations are undeniable and pervasive, but they are not without risks, as depicted below.



Emerging Aviation Risks | By-products of Innovation

	Electronic Flight Bags (EFBs) - Tablets	ACARS	Automatic Dependent Surveillance Broadcast (ADS-B)
New Innovation	Contains tools to automate tasks such as weight/balance, track routes with weather overlays. Replaces traditional paper maps and other manuals.	Text-based, ground-to-air communication that indicates everything from a plane's location (on/off ground) to flight plans and weather information to maintenance data.	Air traffic surveillance technology, which is part of the NextGen Air Transportation System, requires no pilot input and utilises satellite technology for an aircraft to periodically broadcast its position for tracking.
Associated Risks	Unintended exposure when a pilot uses a tablet to download email, browse the web, or update the EFB in hotel rooms – potential impacts include flying through dangerous weather, flight delays, or aircraft risk due to weight/balance issues.	ACARS data is neither encrypted, nor authenticated. Potential impacts include sending wrong information about a plane's location, inaccurate status of maintenance and unreliable data regarding weather conditions.	Data can be 'spoofed' or 'jammed' to create ghost flights, alter apparent trajectory of planes currently in-flight and delete planes from screens, also creates potential to jam ground-based radar, which could affect the ability to control traffic in high-density areas.

[2] Wikipedia.org, Aircraft Communications Addressing and Reporting System, http://en.wikipedia.org/wiki/Aircraft_Communications_Addressing_and_Reporting_System, (Mar 21, 2015).

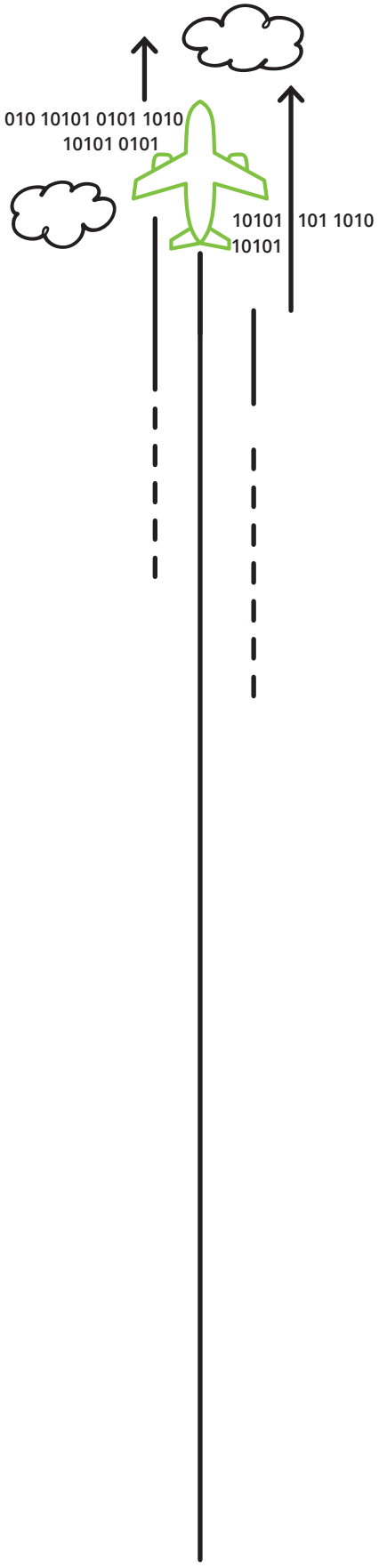
The new Boeing's 787 Dreamliner, Airbus A380 as well as the new A350XWB Airbus, are already digitally enabled. Older generations of commercial aircraft such as legacy Boeing 737 and 777 models, as well as the Airbus A320 family, are being retrofitted with these capabilities. These modern commercial aircraft have essentially become flying industrial control systems – remote, computer-controlled devices that transport millions of people daily for both business and leisure travel. Each aircraft operates as a complex and potentially hackable, infrastructure of interconnected information technology systems, relying on fly-by-wire and legacy ground-to-air systems to provide flight instructions, identify aircraft weight and balance issues, locate other planes and avoid dangerous weather.

Traditional threats remain

The industry is still exposed to more familiar cyber-risks. E-commerce is the aviation industry's primary sales platform. With the development of sophisticated online sales channels and rewards programmes, airlines have become increasingly reliant on internet-based data exchange to transact and promote their organisations. Airlines sell a large portion of their tickets directly to customers, avoiding third party Online Travel Agencies (OTAs) altogether. Loyalty programme IDs and payment card information (PCI) are used to link consumers to their reservations and may be stored and accessed by a range of other services, including executive club memberships, seat upgrades and baggage check-in services, across a range of devices like in-airport kiosks, consumer handheld devices and gate agent kiosks. A gate agent or automated kiosk can access a customer's entire profile and itinerary using one piece of personal identification information (PII). A cyber breach involving a single identifier, or a rudimentary social engineering attack, opens the possibility that a malicious actor could find out exactly where individuals are traveling to and from, when they will arrive and even which gate they will be arriving at. In the hands of a spy, a stalker, or a kidnapper, this information could threaten passenger safety and expose airlines to new sources of potential liability. Airlines are already dealing with impersonation of frequent flyer accounts and the theft of loyalty programme points. On top of that, they struggle to continually balance the ease of experience with the application of typically non-consumer friendly security controls.

Aviation as critical infrastructure

South Africa needs to start looking at international trends as a future direction to assist with improving critical infrastructure cybersecurity, which has identified aviation as a critical infrastructure sector. The order directed at the National Institute of Standards and Technology (NIST) to work with stakeholders to develop a voluntary framework, based on existing standards, guidelines and practices, to reduce cyber-risk to critical infrastructure. A year later, NIST released its first version of the "Framework for Improving Critical Infrastructure Cybersecurity," which provides a prioritised, flexible, cost-effective and repeatable approach to managing cybersecurity-related risk. While the Government's prioritisation of aviation has helped shine a spotlight on the sector and has begun to stimulate important discussion, many questions remain about what a comprehensive and effective programme looks like in both design and practice for commercial airlines.

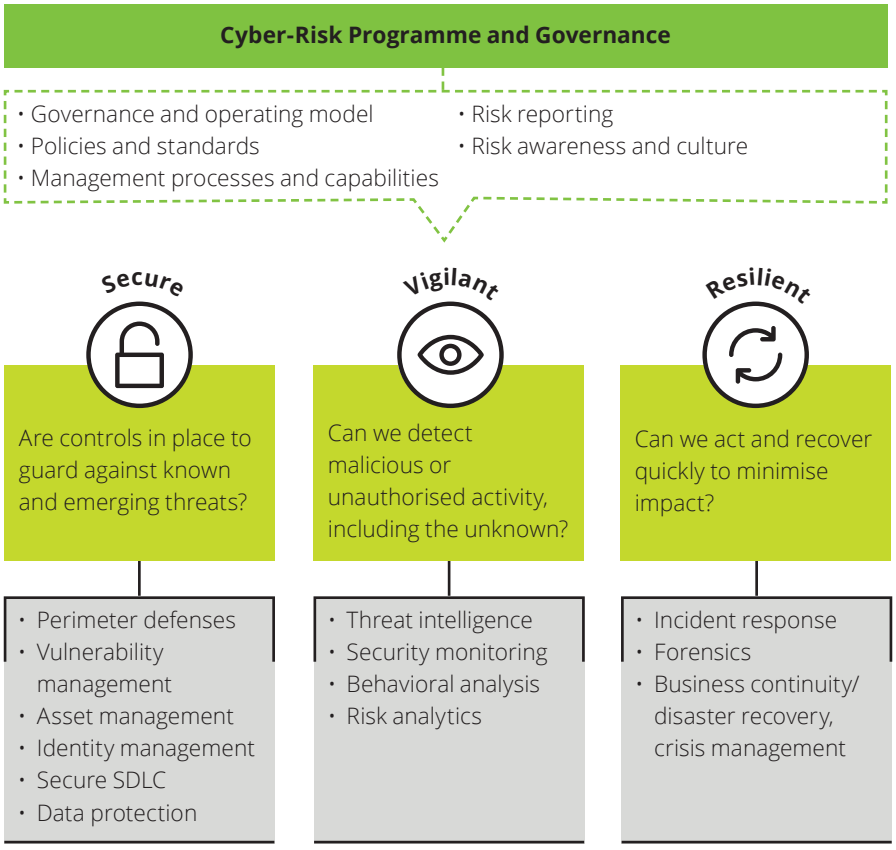


Getting ahead of the new threats

An effective cyber-risk programme should consider the unique set of cyber threats to which the organisation is exposed, or cyber threat landscape, to set realistic goals that can and should be achieved with a broad, well maintained cyber-risk framework. No environment is completely secure, nor is it cost effective to try to make it so. An organisation should not only take reasonable steps to protect its data, applications and infrastructure, but should also minimise the damage of successful attacks and return to normal operation as soon as possible.

To effectively manage cyber-risk, an organisation must be:

- **Secure:** Protect critical assets against known and emerging threats
- **Vigilant:** Maintain threat awareness and detect adversarial activity
- **Resilient:** Recover quickly when incidents occur



Who?

Who might attack?

- Cyber criminals
- Hacktivists (agenda driven)
- Nation states
- Insiders/partners
- Competitors
- Skilled individual hacker

Why?

What are they after and what are the key organisational risks that need to be mitigated?

- Theft of intellectual property or strategic plans
- Financial fraud
- Reputation damage
- Business disruption
- Destruction of critical infrastructure
- Threats to health & safety
- Loyalty rewards programme fraud
- Fuel hedging tactics disruption
- Schedule management algorithm disruption
- Terrorism

How?

What tactics might they use?

- Spear phishing, drive by download, etc.
- Software or hardware vulnerabilities
- Third party compromise
- Multi-channel attacks
- Stolen credentials
- Brute force attack
- Kiosk fraud
- … and others

Secure

Protection against known and emerging threats across the ecosystem

An effective security programme should continually innovate to protect critical assets against known and emerging threats across the organisation. While it may not be possible to eliminate the use of credit card numbers to identify reservations, airlines can utilise tokenisation technologies to avoid proliferating data such as credit card numbers, known traveller IDs and passport numbers throughout the environment. Consumers demand a mobile experience for boarding passes, to change seats and request upgrades, to book reservations and for myriad other, authenticated interactions. Public Key Infrastructure (PKI) technologies may be used to encrypt mobile traffic and automate authentication for consumers, increasing security of mobile transactions transparently to the consumer experience. Business units are rapidly partnering with third parties for various services, requiring that vendors have access to specific IT assets. Federation technologies enable business partners to securely access resources without the organisation exposing sensitive internal directories or taking on the burden of managing third-party identities and credentials.

Vigilant

Pre-emptive visibility and situational awareness

Breaches will occur; preventing successful attacks is no longer as simple as patching systems and updating intrusion detection signatures. The ability to rapidly identify attacks is essential in containing the damage they can inflict. A cyber intelligence centre that is integrated into both sensitive applications for detection and security technologies, such as identity management and network access control, for control is the core of an organisation's ability to be vigilant for and respond to cyber threats. To be truly effective, the CIC needs to be supported by a Cyber Incident Response Team (CIRT), which monitors, assesses and escalates incidents. The CIC also continuously refines use-cases to reduce false positives and to optimise log storage for capacity and forensic analysis. In many cases, the CIC can identify emerging threats based on advanced threat intelligence from multiple industry, law enforcement and other governmental information sharing and analysis centres (ISACs). Non-profit organisations such as the Aviation Information Sharing and Analysis Centre (A-ISAC) are designed specifically for this purpose by providing industry-focused functions to protect aviation organisations, operations and services globally.

Resilient

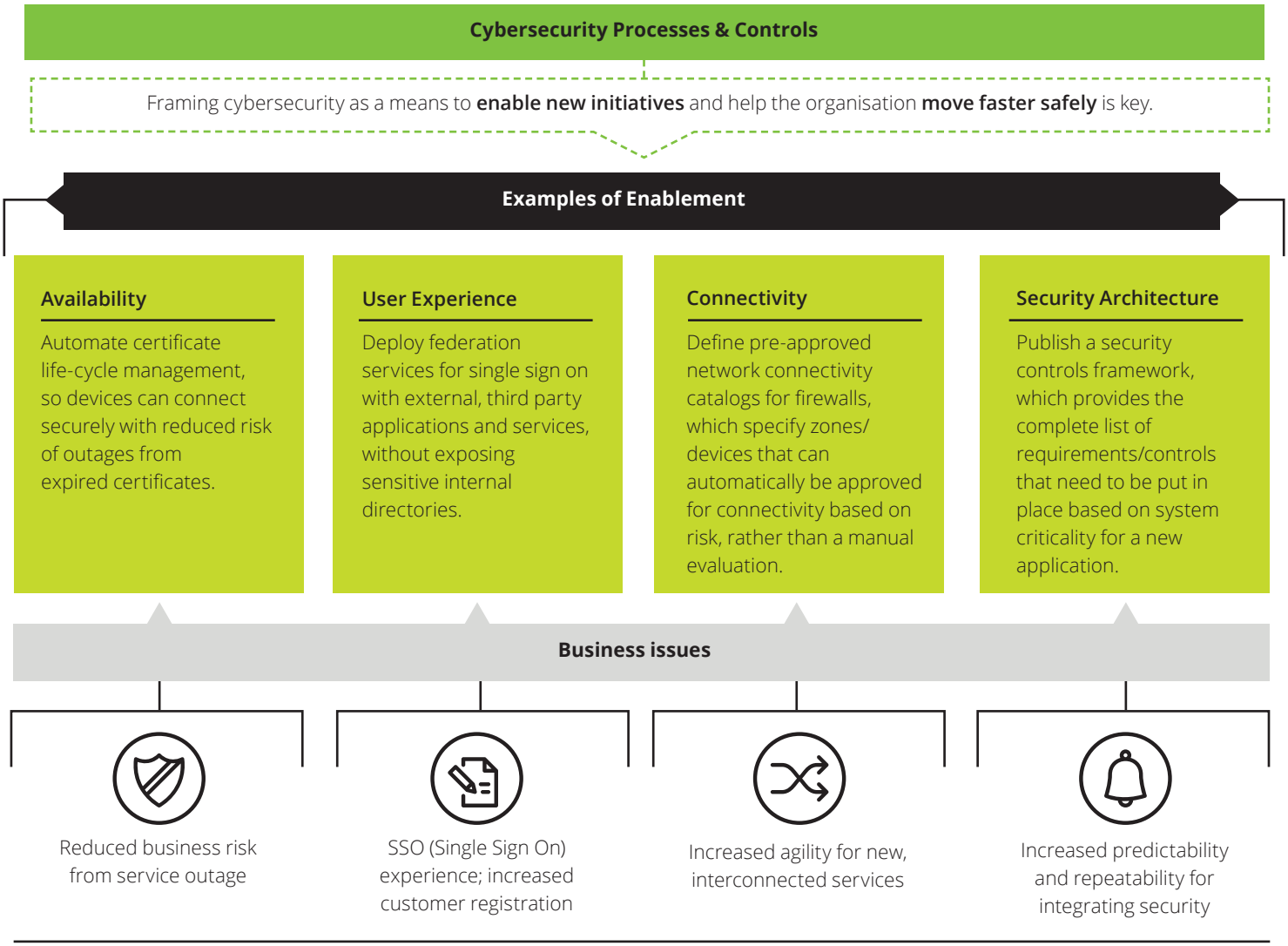
Capability to recover when incidents occur

Given the nature of the organisation and inherent risks to passenger safety, the majority of airlines are well-versed in incident response and crisis management. However, the threats that cyber attacks pose are far different and in some cases, far more complex, than the traditional safety issues that the aviation industry has experienced and beyond what many are prepared for. Airlines can prepare for these new threats by rehearsing response to attack scenarios through cyber-war gaming. Cyber-war gaming involves "tabletop exercises" that emulate actual and possible cyber threats to an organisation to understand how effectively the organisation responds. These exercises involve all levels of the organisation, including organisational leaders, technical teams, legal counsel and external parties such as law enforcement and independent third parties, to assess how effectively they interact to manage what can often be substantial ongoing business recovery efforts. Typically, the greatest shortcomings exposed during these exercises are lack of familiarity and preparedness by executive teams and lack of a coordinated response across the many functions within the organisation.

While it may not be possible to eliminate the use of credit card numbers to identify reservations, airlines can utilise tokenisation technologies to avoid proliferating data such as credit card numbers, known traveller IDs and passport numbers throughout the environment.

Make the business case to position cyber-risk efforts as enablers

An effective and funded secure, vigilant and resilient cyber programme must have visibility at the C-suite level. Cyber-risk is an organisational risk and must be considered when an airline evaluates its overall enterprise risk to make organisational decisions. Savvy Chief Information Security Officers (CISOs) and Chief Security Officers (CSOs) are able to position their cyber-risk programme as an enabler, rather than purely as a necessary evil to maintain compliance. Each investment should have an associated business case, with clear identification and quantification of both enterprise risk reduction and organisational benefits, which may include for example, improvements in customer experience, operational efficiency through automation of provisioning and governance processes, avoidance of costly, mandated security controls for sensitive data through tokenisation technologies and providing greater agility to support partnering with external vendors.



The financial benefits can be direct; for example, insurers provide a material break (discount) on cyber insurance for well-developed security programmes – cost savings that flow directly out of general and administrative expenses and go straight to the bottom line.

In a highly concentrated and heavily competitive industry like aviation, where everybody is seeking new technology to improve efficiency, margins and customer experience, the goal of a robust cyber-risk programme is to enable an organisation to move faster, safely. Such a programme not only facilitates, but can accelerate, business initiatives by ensuring that the appropriate processes and procedures are in place for mainstream enterprise adoption and implementation of new technology.

Take it to the top – executive sponsorship and corporate governance is key

Cybersecurity should have a seat in every meeting of the board to discuss cyber-risk in the context of enterprise risk. The board should understand cybersecurity and meetings should include regular and consistent reviews of cyber-risks along with the overall state of security. Another leading practice is the formation of a 'risk management committee' that comprises multi-functional department heads, including internal audit, flight operations, insurance, legal and information security, that meet regularly to discuss cyber-risk.

The cyber-risk programme as the "seatbelt" for organisation innovation

Traditional threats remain, but as the aviation industry reaps the rewards of technology innovation, the industry must also respond to an emerging and ever-evolving array of cyber-risks. The consequences are no longer limited to data privacy breaches and compliance penalties. In the worst cases, cyber-risks can threaten passenger safety and ultimately the viability of the organisation itself. While cybersecurity is viewed by many as a 'necessary evil' that slows down progress, it does not have to be that way.

A seatbelt analogy is apt: the seatbelt provides an additional safety layer to enable faster travel. Likewise, investing in a robust cyber-risk programme enables the organisation to continue to compete and grow through technology innovation, but also address the associated risks. For aviation organisations, where the network now includes planes and the passengers they carry: "Are you really doing enough to protect your network?"

Contacts

Southern Africa

Navin Sing
Managing Director: Risk Advisory Africa
Mobile: +27 83 304 4225
Email: navising@deloitte.co.za

Shahil Kanjee
Risk Advisory Africa Leader: Cyber & Technology Risk
Mobile: +27 83 634 4445
Email: skanjee@deloitte.co.za

Henry Peens
Associate Director: Risk Advisory Africa
Mobile: +27 82 496 8694
Email: hpeens@deloitte.co.za

Central Africa

Tricha Simon
Risk Advisory Regional Leader: Central Africa
Mobile: +260 973 224 715
Email: tsimon@deloitte.co.zm

Rodney Dean
Director: Risk Advisory Central Africa
Mobile: +263 867 700 0261
Email: rdean@deloitte.co.zw

West Africa

Anthony Olukoju
Risk Advisory Regional Leader: West Africa
Mobile: +234 805 209 0501
Email: aolukoju@deloitte.com.ng

Temitope Aladenusi
Director: Risk Advisory West Africa
Mobile: +234 805 901 6630
Email: taladenusi@deloitte.com.ng

East Africa

Julie Nyangaya
Risk Advisory Regional Leader: East Africa
Mobile: +254 720 111 888
Email: jnyangaya@deloitte.co.ke

William Oelofse
Director: Risk Advisory East Africa
Mobile: +254 20 423 0000
Email: woelofse@deloitte.com

Deloitte.