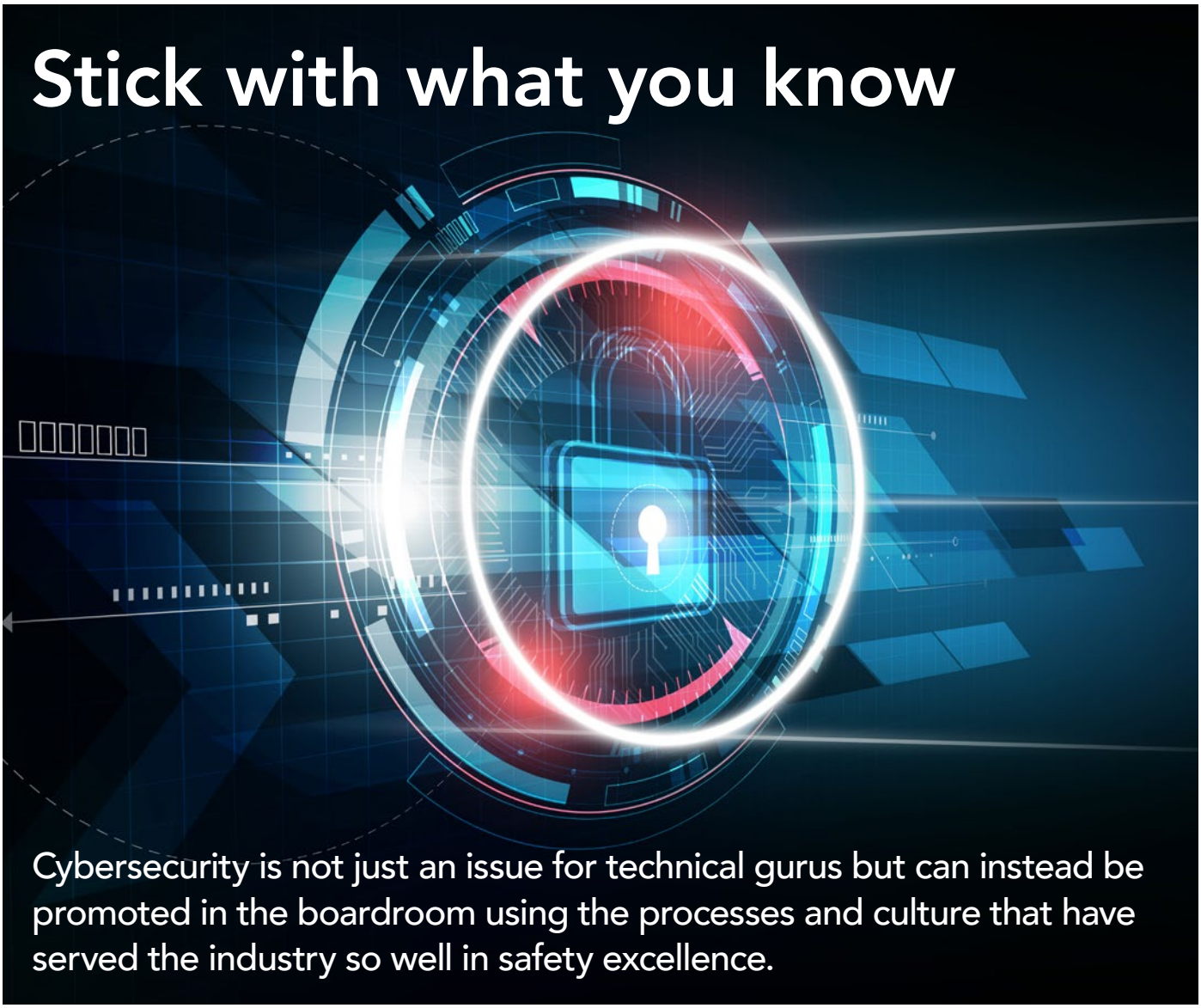
Stick with what you know



Credit: iStock.com/ChakisAtelier

Cybersecurity is not just an issue for technical gurus but can instead be promoted in the boardroom using the processes and culture that have served the industry so well in safety excellence.

Aviation cyberattacks are increasingly common. The European Aviation Safety Agency (EASA) estimates there are 1,000 attacks every month on aviation systems worldwide.

Moreover, the sophistication of these incidents is on the rise. A first generation saw attacks on the availability of systems. Now, a second generation is interfering with the integrity of data within systems – a far more insidious occurrence.

Air traffic management, like every other element in the aviation value chain, is vulnerable to cyberattacks. A number of recent improvements to safety and efficiency in ATM also bring with them the need for greater cyber resilience.

These improvements include the communication shift between tower and aircraft from voice to data, electronic flight strips – which support the automatic generation of clearance messages – and evolving concepts such as D-TAXI – which enables data communication during taxiing.

Meanwhile, automatic dependent surveillance – broadcast (ADS-B) on aircraft and ground vehicles depends on a signal that can be received by hackers on inexpensive equipment, providing an extremely accurate portrait of airport operations for anybody planning a physical disruption.

Perhaps most significantly, system-wide information management (SWIM) and remote/digital air traffic control towers carry with them not only enormous benefits but also greater exposure to cyber threats.

CANSO recently issued a working paper to the ICAO 13th Air Navigation Conference on *Cyber Resilience in the SWIM Concept*, which called for a commitment to cybersecurity governance for all phases of SWIM development and deployment. "This has to be included in all relevant ICAO Standards and Recommended Practices," says the paper, which was accepted by States at the Conference.

The paper also advises:

- States and operators to promote a security culture for all actors in aviation, including publishers, internal/external users and international users
- ICAO to create guidelines for States that will define a clear matrix of roles and responsibilities to ensure that the protection layer is proactively managed and even weak signals of potential acts of unlawful interference can be captured, analysed and managed
- States to create contingency plans based on a local and international risk and threat approach to mitigate disruptions within the system as a result of cyber-attacks or cyber failures.

Cultural shift

The industry continues to work diligently to mitigate the damage caused by hackers. But a cultural shift is required to complete cybersecurity concepts.

Speaking at AVSEC World Day in October in Athens, Leen van Duijn, KLM's Vice President, Security Services, said: "Cybersecurity is not a boardroom topic in general. It is mentioned but without sufficient knowledge. And the fact is that every day brings another new challenge."

Because there is a lack of understanding at the boardroom level, it is hard for organisations to judge how much to invest in cybersecurity and what are the main vulnerabilities.

The problem is compounded by scant collaboration and an abundance of regulatory bodies. The former is frequently overlooked as companies often share information but rarely share best practice. The latter obscures global standards making cybersecurity hard to implement and even harder to benchmark.

Processes and partnerships

But an effective cybersecurity culture might be within touching distance for most aviation companies, including ANSPs. The industry is already wrapped in safety and security values. Utilising these values is a must to improve cyber resilience and achieve the necessary balance between operational efficiency and good cybersecurity.

Stefan Galler, Director ATM Networks, Frequentis, says that ANSP cybersecurity is a business challenge that requires organisational and technical measures to be successfully overcome. Fundamental to success are the processes and partnerships that the industry know well.

> ANSP leaders should view investment in cybersecurity in the same terms as they view investment in safety, where there is no measurable return on investment. If the investment was enough, you don't have a measurable return, since nothing happens.

"Different models for collaboration are possible and the work can be split in different ways," he says. "Making sure you are aware of potential threats and can allocate available resources to continue business is key."

Much as safety is constantly checked and verified, a security health check on technical and administrative levels should be performed at regular intervals, says Galler, "together with system vendors and a knowledgeable consultant who can demonstrate experience in the fields of safety and security as well as in IT".

Similarly, technology partnerships with dedicated security technology providers should be established to focus on solving specific challenges, including mobile device security, advanced authentication and sophisticated cryptography.

Credit: iStock.com/gorodenkoff

Making sure ANSPs are aware of potential threats and can allocate available resources to continue business is key.

Credit: iStock.com/solarseven

Cybersecurity is a constant risk for all industries...the focus should be on situational awareness and business continuity.

"To protect against telephony denial of service attacks (TDoS), partnerships need to be established between public safety answering points and telecom operators who are responsible for delivering emergency calls and who can filter out a flood of fake calls causing denial of service," says Galler.

TDoS can affect a vital communication tool in the ATM armoury and are also often used in conjunction with another cyberattack – so that information about that other attack is harder to distribute.

Galler advises that ANSP leaders should also view investment in cybersecurity in the same terms as they view investment in safety. How much an ANSP should spend on cybersecurity "is a business decision, one regarding business continuity and situational awareness," he says. "But there is no measurable return on investment. If the investment was enough, you don't have a measurable return since nothing happens."

Conversely, of course, invest too little, and the consequences could be catastrophic.

"Cybersecurity is a constant risk for all industries that cannot be won," concludes Galler. "Keeping technical systems secure once they have been put into operation is a day-to-day management task requiring collaboration to carry out things like cyber risk management, monitoring security warnings, applying patches, managing accounts, maintaining firewalls and detecting intrusions.

"Therefore, the focus should be less on avoiding or defending but more on situational awareness and business continuity. It is of common interest to apply due care and keep systems safe and secure."

The CANSO Cyber Security and Risk Assessment Guide is available to download from the CANSO website.

Technology partnerships with dedicated security technology providers should be established to focus on solving specific challenges, including mobile device security, advanced authentication and sophisticated cryptography.

Constant checks

ANSPs are naturally at varying levels of cybersecurity readiness due to the differing levels of openness in their systems. Many still have closed, siloed systems where the need for cybersecurity is obviously different than for open, converged IT systems.

"Today, many clients operate legacy systems which were designed and procured years ago," says Stefan Galler, Director ATM Networks, Frequentis. "Although these systems may still provide up-to-date functionality and productivity, the landscape of cyber threats and the solutions for defending systems have changed. If the security of these systems has not been continuously updated and security collaboration has not been implemented, then we advise doing a security health check."

Constant re-evaluation – whatever the state of preparedness – is therefore a fundamental of cybersecurity.