The goal for global aviation is to become a “system of systems”, with all relevant air traffic information shared seamlessly to support collaborative decision-making.

The major ATM modernisation programmes – Europe’s SESAR, NextGen in the US and Japan’s CARATS – have all been designed with this in mind. These programmes invariably demand greater information sharing through the increased use of common networks and standards.

While there are clear benefits to this approach, it makes ATM increasingly vulnerable to cyber attack. And the potential damage a successful cyber attack would cause is devastating:

• It could be sufficient to close the skies to air traffic for prolonged periods.
• It could lead to “knock-on” failures across connected systems or common components.
• It could erode trust in new systems and concepts, potentially limiting their successful deployment.

“Countering the threat of cyber attacks must be a collective top priority,” says Jeff Poole, CANSO’s Director General. “One of our most important duties as an industry is to preserve and defend the aviation value chain against anything that puts the aviation eco-system at risk.”

Coherent and consistent

The mutual dependence of each player in the aviation value chain makes partnership the cornerstone of a successful cyber security strategy.

“Organisations must be able to trust their partners not to introduce vulnerabilities or new threats,” Poole notes. “We are only as secure as our weakest link. Each of us therefore owes it to the other industry partners to take every step possible to ensure the integrity of our systems.”

ANSPs, working through CANSO, have recognised this fact and a positive start has been made.

The Civil Aviation Cyber Security Action Plan and accompanying roadmap, for example, has been signed by several industry associations alongside CANSO, including ICAO. The goal of the Action Plan is to ensure that all industry stakeholders promote a
coherent and consistent approach to cyber security. An Industry High-level Group is working with ICAO to develop collaborative approaches to cyber security and will present a progress report to the 39th ICAO Assembly in September 2016.

The report will contain a set of recommendations for the industry and regulators. “It is hoped that, through ICAO, we can encourage the adoption of international standards and industry best practices and help build trust in networks and information sharing mechanisms so that all stakeholders will have confidence in the security of the global aviation system,” says Poole.

CANSO has also produced specific guidelines for the ATM community. The Cyber Security and Risk Assessment Guide contains such practical guidance for ANSPs as conducting a cyber risk assessment as a first step to understanding and managing the vulnerabilities in systems, assets, data and capabilities.

It recommends that ANSPs identify the key assets that need to be protected and develop resiliency in case of cyber attack.

CANSO is further disseminating its recommendations on cyber security through workshops and sharing best practice. And there is also the industry-wide information-sharing and analysis centre (ISAC) concept, now being implemented in the US and Europe.

This allows intelligence about threats and risks to be shared in a secure and confidential manner and is another move in the right direction.

A new approach

Matt Shreeve, Senior Consultant at Helios, warns that while partnership underpins the answer to the cyber threat, it is not a magic bullet that can overcome all cyber security challenges.

“A strategy has to be agreed that can keep the industry ahead of the hackers. Shreeve champions a new approach that ensures the development and implementation of appropriate security layers from the outset. This way, aviation can avoid the mistakes made in other industries when technology was assumed to be the only answer.

“The foundation needs to be a corporate policy and management system as cyber security is as much an organisational issue as a technical issue,” Shreeve says.

“Knowing your critical operational and business functions and assets, their connectivity and exposure, and your own risk-benefit tolerance are essential enablers.”

Although this approach is a cornerstone of CANSO’s cyber security recommendations, it is nevertheless a challenging proposition.

To begin with, understanding assets and information flow is a multi-disciplinary activity. There are operational, strategic and technical perspectives to consider – this is not just an IT problem and must involve the whole organisation.

And then, once assets have been identified, they can be no the loss of that asset would have – such as loss of real-time flight information or communication functions.

It can be a very complex calculation that depends on many factors, not least the extent of the threat. And the latter is an x-factor that makes it very difficult to judge appropriate responses and resource allocation.

Ultimately, the provision of end-to-end services usually involves a broad range of assets, which is why they need to be studied and evaluated before a cyber security strategy is put in place.

Make it law?

Matt Shreeve, Senior Consultant at Helios throws an interesting question into the cyber security debate: should the disclosure of a cyber attack be made obligatory for the aviation community?

“The probability of attack on a network can only be accurately assessed if attacks on neighbouring networks are known,” he says. “However, cyber incident reporting is poor in aviation at the moment, meaning risk assessments are often guesswork. Improved disclosure and reporting will therefore help by providing better statistics.”

“Disclosure laws in other industries and countries support this: the media impact of new stories eventually drops off, so the ‘shaming’ effect attenuates even as the evidence base for improved cyber security improves.”
Shreeve makes it clear that cyber security strategy shouldn’t start with building in layers of technology safeguards. “Firewalls are almost the last piece of the cyber puzzle!” he counsels.

A sense of control

Indeed, one argument suggests firewall are not sufficient on their own. Detection as well as protection is becoming the new mantra. The reasoning is simple: detecting brings back the advantage to the good guys.

A hacker is looking for just one vulnerability. And that vulnerability only needs to be exploited once. System defences, on the other hand, have to be designed to protect everything 24/7. In other words, attacking is cheap and easy, defending is costly and difficult.

But if detection as well as protection is emphasised, an organisation can begin to regain some sense of control. Any hacking attempts could be quickly identified through constant monitoring, potentially enabling the source of the attack to be traced and generating critical information.

This is not to say that firewalls are not needed or that cyber security can be achieved cheaply.

A specific threat

CANSO is addressing specific cyber threats. A case in point is the CANSO task force on automatic dependent surveillance – broadcast (ADS-B) security, which has been studying the security vulnerabilities in the technology with a view to recommending solutions or defensive measures.

Its work typifies the challenge of vulnerability facing ATM. Many of the traditional communications, navigation, and surveillance (CNS) and ATM systems were designed for operational excellence and so have open unencrypted technology whereby data, including aircraft ID, altitude, position, bearing and speed can be received by any airborne or ground-based receiver.

As Shreeve puts it: “Cyber security is the cost of doing business in the modern, interconnected world. We know there is a cost if passengers lose trust in the aviation system.

“Cyber security is a challenge, but one that can be addressed cost-effectively if the industry works together,” he concludes.

The Air Traffic and Navigation Services SOC Limited (Reg No 1993/004150/06) (ATNS) provides air traffic services throughout the country and is responsible for the provision of the system infrastructure necessary to ensure a safe and effective service.

Appointment of an External Aviation Safety Expert who will Provide an Independent Review of the Safety Management System (Plus All Its Processes) and Ascertain what Management Interventions are Adequate to Address Air Traffic Management Safety in Line with Best Practices

Reference No: RFQ/SRA/25/11/2015

The RFQ/SRA/25/11/2015 document is downloadable from the ATNS website: http://www.atns.co.za or available electronically on request, in Word format, between 09:00 and 16:00 (CAT) daily from 30 November 2015 to 14 January 2016 from ATNS Head Office, Eastgate Office Park, Block C, South Boulevard Road, Bruma, 2198, Johannesburg, South Africa.

The closing date and time for the submissions of proposals is 15 January 2016 at 16:00 (CAT).

Proposals are to be submitted in the tender box, Reception, Ground Floor, ATNS, Eastgate Office Park, Block C, South Boulevard Road, Bruma, 2198, Johannesburg, South Africa.

Printed and bound documents of the proposal, 1 (one) original hard copy and 2 (two) copies; and 1 (one) electronic copy (on CD/memory stick) in PDF format are required (delivered to the reception). No proposals forwarded by telegram, telex, facsimile, e-mail or similar medium will be considered. Late applications will, regretfully, not be accepted.

Tender responses sent by post or courier must reach this office at least 36 hours before the closing date as specified, to be deposited into the tender box. Failure to comply with this requirement will result in the proposal/tender response being treated as a “late proposal/response” and will not be entertained. Such proposals will be returned to the respective bidders.

To request application documents and additional information, please contact the Procurement Specialist, Jean Makaya-Moyane, tel. (011) 607-1158 or via e-mail: JeanM@atns.co.za

Closing date: 15 January 2016