THE IMPORTANCE OF EFFECTIVE CYBERSECURITY CULTURE

Photo Credit: Philipp Katzenberger on Unsplash

Rashad Karaky

Aviation Cyber Security Officer, ICAO

Author details

Rashad Karaky has been working in the civil aviation sector for more than 15 years. He is a computer scientist by training with a specialization in software development. In the aviation industry, he managed several aviation domains for the Arab Air Carriers' Organization, a regional airline organization in the Middle East and North Africa, including economics, safety, aviation security, cybersecurity, facilitation, emergency response planning, Air Traffic Management and airspace infrastructure, and engineering & maintenance. He joined ICAO in August 2020 in the role of Cybersecurity Officer in the Aviation Security Policy Section, a role in which he supports the development of a global, robust, and sustainable cybersecurity framework for the international civil aviation sector.

Introduction:

In support of the **Year of Security Culture 2021**, we should consider the importance of **cybersecurity culture**, as an integral part of security culture in aviation.

To provide an analogy with the physical world, one of the benefits of security culture is to help raise awareness of the key role of human factors. This complements technical means, as well as better protecting against insider threats, i.e. people inside the system collecting information with the intent to cause harm to assets and/or lives. Cybersecurity culture would similarly help protect against a different kind of insider threat: an intruder or a malware lurking within the organization's infrastructure, watching, stealing sensitive information, and/or waiting for the right moment to cause harm to our aviation assets and/or lives. We may not be able to see cyber threats, and this is exactly what makes them more insidious than physical threats. And it is why ICAO, and indeed all aviation stakeholders, are actively addressing cybersecurity in civil aviation.

Cybersecurity scope

Cybersecurity gained prominence in the air transport sector over the past couple of decades. The interconnection of systems and networks, and the data sharing between multiple systems and stakeholders, required a cross-domain cybersecurity approach for the aviation community. That approach allows the sector to identify cyber threats, protect itself through mitigating those threats, detect cyber events when they take place, prepare for and respond to those events while recovering and ensuring the continuity of operations.

Accordingly, a broad definition of cybersecurity is the following: **It is the collection of people, processes, and technologies deployed to identify, protect, detect, respond to, and recover from intentional and/or unintentional cyber events that may jeopardize organizations and users' assets, and that may affect agreed levels of safety, security, and continuity of civil aviation operations**.

Cybersecurity and ICAO

The discussion of cybersecurity in ICAO began in the early 2000's, in parallel with the discussion of new air navigation concepts and the need for information security to protect the flow of data between the different stakeholders involved with the operation of the aircraft (i.e. operators, airports, air navigation service providers, etc.). As the civil aviation sector's reliance on information and communication systems increased over time, there was a requirement to ensure the availability, confidentiality, and integrity of data. As a result, several cyber-related initiatives took place in ICAO, and discussions over cybersecurity evolved to cover the whole air transport sector. Those discussions led to the adoption of two ICAO Assembly Resolutions: Resolution A39-19, superseded by Resolution A40-10. The latter paved the way to the development of the Aviation Cybersecurity Strategy, and the later endorsed the Strategy and requested ICAO to develop a roadmap for its implementation.

The Aviation Cybersecurity Strategy

The **Aviation Cybersecurity Strategy** is a translation of ICAO's cybersecurity vision for the global civil aviation sector to be resilient to cyber-attacks, safe and trusted globally, whilst continuing to innovate and grow. The Strategy is a framework built over seven pillars:

ICAO

Security and Facilitation Strategic Objective

Aviation Cybersecurity Strategy

October, 2019

Approved by and published under the authority of the Secretary General

INTERNATIONAL CIVIL AVIATION ORGANIZATION

- International cooperation
- Governance
- Effective legislation and regulations
- Cybersecurity policy
- Information sharing
- Incident management and emergency planning
- Capacity building, training and cybersecurity culture

The first edition of the **Cybersecurity Action Plan** was published in November 2020. It is a living document that aims at supporting States and stakeholders in implementing the Cybersecurity Strategy. The Action Plan identified 26 Priority Actions which are further broken down into 54 Measures and Tasks, providing the foundation and framework for ICAO, States, and stakeholders to cooperate and work together to address cybersecurity in civil aviation.

ICAO Aviation Cybersecurity training, workshops and seminars

ICAO will continue working in 2021 to develop and deliver Aviation Cybersecurity training, workshops and seminars. These will be based on the newly-developed Cybersecurity Training Roadmap and course outlines that address the specific requirements of the different stakeholders involved in managing cybersecurity risks in civil aviation. At the same time, work is underway with Embry-Riddle Aeronautical University to develop the *Foundations of Aviation Cybersecurity Leadership and Technical Management Programme* for delivery starting in 2021.

Photo Credit: Icons8 Team on Unsplash

Cybersecurity and Security Culture

Going back to the broad description of cybersecurity, people are generally considered the weakest link in the cyber chain, being the first target of bad actors through social engineering and phishing techniques, or being prone to mistakes and responsible for interferences (whether intentionally or unintentionally).

As such, and similar to controls and processes that are in place to protect systems, networks, and data, cybersecurity includes the notion of human firewalls.

Within that concept, **cybersecurity becomes the responsibility of everyone** - starting from the top office and across all levels in the organization.

Where everyone shares the responsibility for cybersecurity, two main outcomes are expected:

Everyone will **use electronic resources responsibly**, in line with established rules and regulations. This is achieved through the buy-in of senior management to 1) develop policies and procedures for the use of electronic resources and periodic revision of those policies, 2) invest in raising awareness of employees, through recurrent training and workshops, 3) test the impact of those efforts through conducting scheduled and unscheduled penetration tests, 4) and promote/establish a cybersecurity culture in the organization where employees are encouraged to report any issues they cause or come across within the cyber environment, and report issues which they perceive as suspicious or abnormal.

On the other hand, employees are also expected to invest time to learn how to responsibly use electronic resources. Employees need to maintain the security of passwords and/or access tools entrusted to them. They should also ask questions when in doubt of what to do, and report any issues they come across as suspicious or unexpected, whether done by self or by others. This reporting responsibility is the essence and ultimate goal of cybersecurity culture. And it is where cybersecurity culture becomes an essential deterrent against cyber threats as the amount of damage that a cyber-attack causes, is directly related to the time elapsed until its detection and the initiation of the response mechanisms.

Conclusions

Instilling well-established safety and security cultures in the aviation workforce, will allow for the prediction, early detection, and effective response to events that may affect operations. Similarly, an effective cybersecurity culture will further support the safety, security, and sustainability of civil aviation in a sector in which data flow seamlessly between interconnected systems and across all air transport stakeholders.