Square de Meeus 37
BE - 1000 Brussels
Belgium

Phone: +32 2 318 28 00
Fax: +32 2 318 28 01

Information paper
March 2021

European Cybersecurity Policy Framework:
Build Resilience

Over the last years, the uptake of *digital technologies* has grown exponentially, which consequently made it one of the key priorities for the European Commission in their European Digital Strategy. Since it is one of the key priorities in the European Digital Strategy by the European Commission, Business aviation is also gradually being immersed into digitalisation and needs to build cyber-resilience.

Becoming cyber-resilient can be done through solid information security management systems and an appropriate approach to cybersecurity. Considering our industry provides a service with safety of life risks, cyber-resilience is a critical first concern for facilitating business continuity, as well as upholding the highest level of safety.

Aviation is a system of systems. It relies on globally interdependent, and interconnected processes, which can lead to potential cyberattacks on various actors at national, regional and international level, and so, a consecutive increasing number of security vulnerabilities to detect, test and tackle. Information sharing, clear global vision and international cooperation are key tools to enable the necessary resilience to cyberattacks and cyberthreats.

Aviation decision-makers at global level as well as national level are taking steps to deal with the need to protect aviation's critical infrastructure, information and communication technology systems and data against cyber threats. The EU already set up horizontal legislation addressing cybersecurity challenges, covering critical infrastructure sectors, including large aviation stakeholders.

On top of this, the Aviation Security regulatory framework was also reviewed to transpose ICAO's requirements for cybersecurity. EASA is also preparing rules to tackle the safety aspects of information security risks. And so, even though European cybersecurity legislation has been in place for some time, (some) aviation stakeholders are not fully familiar with it.

EBAA has developed this information paper to raise awareness and summarise the current and future European cybersecurity policy landscape for Business aviation.

Cybersecurity Strategies

The International Civil Aviation Organisation (ICAO) acknowledged the importance of protecting civil aviation's critical infrastructure, information and communication technology systems and data against cyber threats. It amended Annex 17 – Security which now includes a Standard and a Recommended Practices on measures relating to cyber threats (4.9.1 and 4.9.2). ICAO developed an ICAO Aviation Cybersecurity Strategy and its associated "Action Plan" which were recently approved. The Action Plan provides a detailed and stepped approach on how Member States and industry must work together and develop a cybersecurity policy, information sharing capabilities, effective legislation, capacity building, governance & accountability. The Action plan is a living document that will evolve with the changes in cybersecurity. A European Strategy for Cybersecurity in Aviation was also developed in 2019 facilitated by EASA with input from the whole aviation industry. Both strategies demonstrate

Square de Meeus 37
BE - 1000 Brussels
Belgium

Phone: +32 2 318 28 00
Fax: +32 2 318 28 01

that cybersecurity requires a holistic and integrated approach at the policy level as well as at the company level to ensure coherence among the various management systems (Safety Management System, Security Management System and Information Security Management System).

The European Regulatory Framework

The European cybersecurity policy paves the way towards a smooth implementation of new cybersecurity requirements. It currently is based on different pieces of legislation at horizontal and sectorial levels. The European Commission is working to increase the efficiency of the regulatory framework.

The first European horizontal legislation addressing cybersecurity challenges is the Directive on Network and Information Systems (NIS Directive) EU 2016/1148**.** The cybersecurity requirements of this directive apply to entities in various critical sectors, identified by the Member States as 'Operators of Essential Services' (OES). Aviation is one of the critical sectors. As per the current NIS Directive, Member States must identify the 'Operators of Essential Services'. The designated OES must identify the network and information systems that need to comply with the Directive's security requirements and take appropriate measures to:

- manage the risks posed to the security of the network and information systems in the provision of their service;
- prevent and minimize the impact of the incidents affecting; and
- report serious incidents affecting the continuity of the essential service.

The European Commission developed a tool kit to raise cybersecurity awareness. It helps to put the NIS Directive into an overall perspective.

While the focus has been so far on 'large' stakeholders, the NIS directive is under revision and its scope will be extended. It should include all large and medium enterprises in active, "critical' and "essential" sectors, as listed in Annex I of the proposal. In doing so, the Directive excludes from its scope small enterprises which are defined as per Article 2 of Commission Recommendation C(2003) 1422. If the criteria described in this recommendation are not met, any small structure may be targeted by the new NIS Directive, including Business Aviation companies.

The new scope also includes digital service providers. The aim is to address the security of supply chains and suppliers' relationships. This scope is much broader and will encompass more operational stakeholders from the industry (air carriers, airports, etc).

The second main EU legislation laying down cybersecurity policy for civil aviation is Regulation (EC) N°300/2008 laying down common rules and basic standards on aviation security (Aviation Security Regulation or AVSEC Regulation). It lays down common rules and basic standards on aviation security and procedures. It is complemented by Implementing Regulation (EU) 2015 /1998 amended by Implementing Regulation (EU) 2019/1583 which transposes the ICAO Annex 17 Standard and Recommended Practice 4.9.1 and 4.9.2 on cybersecurity. Regulation (EU) 2019/1583 stipulates that operational stakeholders, including air carriers, must *conduct effective security risk assessments relating to their operations and implement measures addressing cyber threats,* but it also contains an obligation for the Authorities to *share relevant information to assist these entities in conducting effective security risk assessments related to, among other areas, cybersecurity.* Stakeholders will have to identify and protect their critical information and communications technology systems and data from cyber-attacks that could affect the security of civil aviation.

Square de Meeus 37
BE - 1000 Brussels
Belgium

Phone: +32 2 318 28 00
Fax: +32 2 318 28 01

The European Commission has developed an Information Note to help Member States and operators in the implementation of the requirements related to cybersecurity.

In its current review of the European cybersecurity policy requirements set up in the NIS Directive, the European Commission sets the scene to foster closer cooperation among Member States to improve the efficiency of the legislative framework.

While the safety aspects of the information security risks are not covered in the NIS Directive or the AVSEC Regulation, the EASA Basic Regulation (EU 2018/1139) extends EASA's area of competence to cybersecurity having safety consequences. EASA is preparing a new set of cybersecurity rules (NPA 2019-07) which will cover all aviation domains and their interfaces and will address the safety impact of information security risks in a comprehensive and standardised manner across all the aviation domains. It will require aviation stakeholders, including Business Aviation, to set up an Information Security Management System (ISMS) aimed at identifying, protecting from, detecting, responding to and recovering from any information security incident. As part of it, and based in the current draft, the organisation, including Business Aviation companies (air operators, aerodromes etc), would be required, among other aspects, to:

- identify its activities, facilities and resources, as well as the services it operates, provides, receives and maintains, which could be exposed, directly or indirectly, to information security risks;
- identify the equipment, systems, data and information that contribute to the functioning of the elements listed in the point above;
- identify the interfaces it has with other organisations, and which could be exposed to information security risks;
- Develop and implement measures to manage the identified risks.

The organisation would also be required to define:
- The lines of responsibility and accountability throughout the company;
- an Information Security Management Manual;
- an internal reporting scheme to enable the collection and evaluation of information security events and vulnerabilities of equipment, process and services. The system should enable a proper record keeping adequate storage, accessibility, and reliable traceability.

EASA attempts to ensure adequate proportionality of the rules and consistency of management systems. In particular:
- the ISMS shall correspond to the size of the organisation and the nature and complexity of its activities;
- the organisation may integrate the ISMS with other management systems it has already implemented.

Member States would have to ensure that the competent authority responsible for the oversight of these new EASA requirements (typically, the Civil Aviation Authority) adequately coordinates with other relevant cybersecurity oversight bodies within the Member State (e.g. performing the compliance oversight against the NIS Directive and against the AVSEC Regulation), in order to:
- coordinate and harmonize implementation policies,
- coordinate and ensure compatibility of oversight regimes and reporting schemes,
- reduce the duplication of oversight activities.

The EASA provisions are still in a draft format but the content should remain within these high-level principles.

Square de Meeus 37
BE - 1000 Brussels
Belgium

Phone: +32 2 318 28 00
Fax: +32 2 318 28 01

Acceptable Means of Compliance (AMC) and Guidance Material (GM) are currently under development. They should ensure proportionality, flexibility and will bring clarity on how the requirements should be implemented and adapted to the complexity of the companies.
EASA intends to shape the AMC and GM to ensure a proportional implementation of the regulation and intends to include references to several industry standards being already widely used by the industry. Use of those standards would not be mandatory, but their use would help organisations in their efforts to meet the new requirements.

Cybersecurity Industry Standards

A standard can be defined as a *"document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context*".[1]
Industry standards are voluntary standards developed by the industry and for the industry. They are usually an agreed set of criteria adopted by the members of a sector. The industry professionals can use them to their full extent or further refine them and generate other equally efficient methods for proving compliance with regulations. In the case of the aviation sector, these newly developed means of achieving compliance can be filed at EASA as Acceptable or Alternate Means of Compliance (AMC / AltMoC).

Cybersecurity industry standards are specifically developed to build the cybersecurity resilience of a user/organisation and of the cyber environment it works in.

The ISO/IEC 27001 Information Security Management System (ISMS) is one of the first standards used in the aviation industry, which provides a holistic management structure to define and resolve information risks and can contribute to independent certification. This is a description of processes in your business and not an IT tool. It consists of targets, tools, definitions of policies and processes.
The National Institute of Standards and Technology (NIST) Framework, established for US Federal use, but widely adopted elsewhere, is another key industry-standard commonly used in aviation.

Information Sharing Mechanisms

Information sharing is an essential building block to set up cybersecurity resilience. Several voluntary information-sharing platforms co-exist so far :

- European Centre for Cyber Security in Aviation (ECCSA) facilitated by EASA;
- European Air Traffic Management Computer Emergency Response Team (EATM-CERT) set up by EUROCONTROL;
- Aviation Information Sharing and Analysis Center (Aviation-ISAC), which is industry-led.

[1] https://www.cencenelec.eu/standards/DefEN/Pages/default.aspx

Square de Meeus 37
BE - 1000 Brussels
Belgium

Phone: +32 2 318 28 00
Fax: +32 2 318 28 01

About EBAA

The European Business Aviation Association (EBAA) is the leading organisation for operators of business aircraft in Europe. Our mission is to enable responsible, sustainable growth for business aviation, enhance connectivity and create opportunities. EBAA works to improve safety standards and share knowledge, to further positive regulation and to ease all aspects of closely tailored, flexible, point to point air transportation for individuals, governments, businesses and local communities in the most time-efficient way possible. Founded in 1977 and based in Brussels, EBAA represents +700 members companies, corporate operators, commercial operators, manufacturers, airports, fixed-based operators, and more, with a total fleet of +1,000 aircraft.

Follow us on Twitter, Linkedin, Instagram and Facebook, or visit our website on www.ebaa.org.