Implications of the new EU Cyber Security Regulations for the Aviation Industry

RAZORSECURE AND VT MILTOPE OVERVIEW

RazorSecure working with Wayra and the GCHQ Accelerator

Table of Contents

Overview

New EU Cyber Security Directives come into force in May 2018 and cover 2 regulations.

- The Network and Information Systems Directive (NIS). Focused on critical infrastructure – Including Airports, Airlines, Rail, Road, Water, Gas, Oil and other critical infrastructure. The regulation mandates 4 key areas – Organization, Protection, Monitoring, Response and Recovery.

- The General Data Privacy Regulations Directive (GDPR) for data privacy and data handling.

The implications of non-compliance are fines of up to 4% of global annual turnover.

Who do these regulations apply to?

- **NIS**

  Airlines – Air carriers as defined in point (4) of Article 3 of Regulation (EC) No 300/2008 of the European Parliament and of the Council.

  Airports – Airport managing bodies as defined in point (2) of Article 2 of Directive 2009/12/EC.

  There are exemptions for smaller airlines and airports, but expect the scope to expand in the future and it is down to each EU member state to define those exemptions.

- **GDPR**

  Any company processing data from EU residents, regardless of company location. Applies to non EU entities.

When will the regulations be implemented?

All EU member states must implement NIS and GDPR by May 2018. NIS includes a 6 month window for governments to identify companies that must comply.

What are the penalties?

For the most serious breaches for companies deemed to be making no attempt to comply with regulations the fines will be the higher of €10m, or 4% of Global Annual Revenue.

For less serious breaches such as not reporting to a local data controller within 72 hours of a breach the fines will be the higher of €5m or 2% of Global Annual Revenue.

The penalties apply to both NIS and GDPR therefore a company could be fined under both regulations.

Potential Vulnerabilities/Risks

Cyber attacks against in-flight Entertainment systems, passenger WiFi systems, passenger information systems, aircraft to ground communication systems, and CCTV systems are all potential targets.

- Access to the systems via engineering port or via wireless connection
- Interception of payments systems data
- Availability of payments systems

- Access to personal data including personal MAC addresses and computer/device identities
- Access to CCTV images
- Access to the electronic flight bag
- Attacks on devices belonging to other passengers
- Attacks on IFE System data and content integrity, for example: changes to content

What are the goals?

The two key goals are defined as follows:

- Securing critical infrastructure from a cyber-attack through bringing critical infrastructure up to modern cyber security standards
- Data privacy as a personal right for every citizen

The goals have evolved from a general improved cyber awareness of the risks and vulnerabilities within industry and the approach that needs to be taken to protect the critical national infrastructure and personal data.

- Cyber security is built around three key tenants, confidentiality, integrity and availability.
- Cyber security is a Board level responsibility and affects all levels of the business
- Cyber security encompasses both physical security, data security and operational security. Whereas the traditional attack on an IT network is aimed at stealing data, money or asking for a ransom it is now recognised that attacks on operational technology (OT) systems, such as aircraft, are aimed at causing disruption, damage, control and brand damage.
- A recognition that security needs, and the threat landscape, change over time, so monitoring, reporting and response are key to a security solution.
- A layered approach is required. Firewalls, VLANs and authentication are not sufficient. Intrusion detection needs to be within the system to protect when the walls have been breached.
- There is a key requirement to monitor, detect, report and protect, as well as to detect changes to “normal” through anomaly detection.
- Regular auditing and testing. Cyber security is not just about keeping systems closed, it is also about integrity and availability of systems.

NIS - The Network and Information Security Directive

Currently being implemented across all 28 member states. There will be slight variations but it is likely all will follow either the UK, France and Germany’s interpretation. The directive also applies to operational systems and must be implemented by May 2018.

The directive covers 4 key areas - Organization, Protection, Security Monitoring, Response and Recovery.

- **Organization**
    - Governance
    - Risk management
    - Asset management and
    - Supply chain

- Using ISO-27001 style requirements

- **Protection**
  - Service Protection Policies and Processes
  - Documented processes
  - Identity and Access Control
  - Documented authentication for individuals with controls
  - Data Security
  - Prevent unauthorized access to data and control data during maintenance/disposal of systems
  - System Security
  - Firewalls, vulnerability management, hardening, software updates, no default passwords etc
  - Resilient Networks and Systems
  - Resilient by design, must consider not only the operation of systems but also the failure management
  - Staff Awareness
  - Staff are first line of defence, appropriate training required

- **Security Monitoring**
  - Must detect actual or attempted breaches
  - More than collection of logs
  - Must be effective for the operational lifecycle of the system
  - Anomaly Detection
  - Detect deviations from "normal"
  - Applies to both network and systems

- **Response and Recovery**
  - Response and Recovery Planning
  - Requires a well-defined and tested incident management process with activities in-place to limit impact
  - Continuous improvement
  - When a breach occurs, steps must be taken to understand the root cause and improvements must be made.

Key points:

- Appropriate capabilities to ensure network and information system security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential services.

- C.1 Security Monitoring:
  The organisation monitors the security status of the networks and systems supporting the delivery of essential services in order to detect potential security problems and to track the on-going effectiveness of protective security measures.

- C.2 Anomaly Detection:
  The organisation detects anomalous events in the network and information systems affecting, or with the potential to affect, the delivery of essential services.

- The Directive requires designated operators of essential services to notify their relevant competent authority or CSIRT of incidents having a significant impact on the continuity of the essential services they provide. *"without undue delay and as soon as possible, at a maximum no later than 72 hours after having become aware of an incident."*

- Active versus Passive
  The traditional approach to cyber security is passive only and uses firewalls, network segregation and authentication. The new cyber directives require active monitoring and anomaly detection.

EU NIS Documents

http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/636207/NIS_Directive_-_Public_Consultation__1_.pdf

GDPR -General Data and Privacy Regulations

GDPR is a new directive from the EU that decrees that data privacy is a right. The directive must be adhered with from May 2018 and applies to data for EU citizens being processed by EU and non-EU entities. The fines for non-compliance are the same as for NIS.

The implications are that a company whose system that is hacked that enables access to an EU citizen's personal data as defined below will be liable to fines.

Importantly these regulations are **extra-territorial**, so they would apply to an EU citizen even if their data was being held in a system outside of the EU.

Personal Data

The EU definition of personal data is much broader than the US definition. It includes anything that can be considered identifiable.

Personal data includes the following:

- Article 2a: 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity;
- Full name, Home address
- Email address
- Social security number / Passport number /Driver's license
- Credit card numbers
- Date of birth
- Telephone number
- Log in details
- A customer number held in a cookie
- An Internet Protocol (IP) address
- A processor or device serial number
- A unique device identifier including MAC address's

The definition also includes CCTV images. These are considered personally identifiable information (PII) under the new regulations and must be protected and only held for as long as necessary and only with permission.

Terms of service should be reviewed to cover use of this data under the passenger WiFi systems. Systems should be checked to ensure data is not stored unintentionally in log files, databases etc.

Potential Vulnerabilities/Risks

All systems that have an interface with citizens, both on and off board.

GDPR Core Principles

- **Consent** must be clearly requested and given, and no 'legalese'
- **Breach Notification** must be reported to each local data controller within 72 hours of a breach and notify customers without undue delay
- **Right to access data.** Data subjects have the right to request all data held on them, this must be provided free of charge.
- **Right to be forgotten.** Data subjects may request removal of their data. This also means that third parties must stop using the data. This can be weighed against "the public interest"
- **Data Portability.** If a subject requests their data, they must get it in a 'commonly used and machine readable format'
- **Privacy by Design.** Data minimization. "Appropriate technical and organizational measures" taking into account "the state of the art and cost of implementation". Ensuring ongoing confidentiality, availability and integrity of systems, restoration of systems in a timely manner after an incident regular testing and assessment of security controls.

EU GDPR Documents

https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

http://www.eugdpr.org/

Additional Cyber Security Considerations

Brand Protection

The impact of a cyber-attack on the value and perceived reliability of a brand is significant and should be considered in parallel with the impending EU cyber regulations.

COPENHAGEN, Denmark (AP) — The world's biggest container shipping line A.P. Moller-Maersk says the June cyberattack that paralyzed its core shipping business is estimated to have cost the company between **$200 million and $300 million**. http://www.businessinsider.com/ap-moller-maersk-cyberattack-cost-up-to-300-million-2017-8?IR=T

The company says the June 27th 2017 malware attack was distributed through Ukrainian accounting software with backdoors into the networks of users. It was contained the following day. The group said its businesses "were significantly affected," but there was "no data breach or data loss."

A new study commissioned by CGI and conducted by Oxford Economics, has found that companies' share prices fall by an average of 1.8 per cent on a permanent basis following a severe breach where large amounts of sensitive data are lost. This means a typical firm is worse off by an average of £120m after a breach, according to the study. It claimed that 52% of British businesses fell victim to

a cyber-attack in 2016, amounting to 2.9 million; they also lost in the region of £29.1 billion in the process.

"Experience shows us that the real threat to UK businesses is not necessarily a fine from the Information Commissioner's Office (ICO). This is a drop in the ocean compared to the bad press and loss of customer confidence that often follows a cyber-hack," Andrew Gilchrist, a senior associate at international law firm K&L Gates LLP.

Safety

Safety is of critical concern. New guidelines have created recognition within the industry that safety and security should be considered together.

Improved cyber security can improve the safety case and particular attention should be given to the following areas.

- Accuracy of GPS. GPS systems can be vulnerable to 'spoofing' which has the effect of providing an inaccurate location. Systems that rely on accurate GPS are potentially vulnerably.
- Avionics systems - Any data connections that may expose a vulnerability into the avionics systems require evaluation and protection.
- DNS Spoofing – Over the air updates and data communication need to be secured against redirection of traffic and man-in-the-middle created by changes to DNS via compromise of DNS servers or a gateway server.

Passenger Protection

There are three key areas where passenger protection could be compromised.

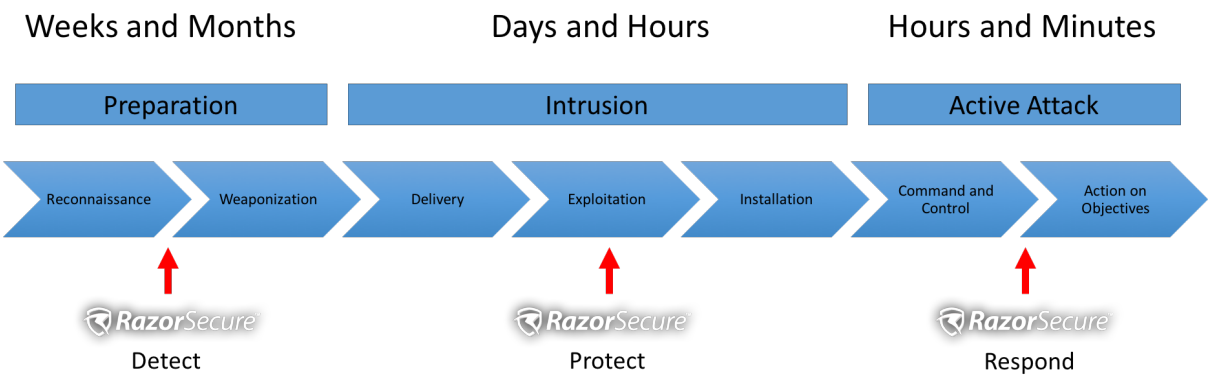
- Access to personal data
  A cyber-attack could gain access to personal data such as MAC addresses, credit card information or CCTV images, all of which come under the GDPR regulations.
- A compromised passenger information system
  There have been several well publicised instances of hackers gaining access to passenger information systems and installing non-company messages. The danger from the installation of a scare message is clear.

Cyber Attacks

A cyber-attack must always go through three key stages which are shown in the Lockheed Martin Cyber Kill Chain diagram – Preparation, Intrusion and Active Attack.

The new cyber regulations focus on anomaly detection to identify attacks earlier in the kill chain to provide an opportunity to prevent attacks before they turn into more serious breaches.

Anomaly detection detects an event that is **not** normal. The event can be reported and, in addition, the ideal scenario is that the intrusion detection cyber solution can also preform intrusion protection that can protect the device and the system with on-device decision making and thus defend against an attack.



The Lockheed Martin Cyber Kill Chain

Network Monitoring versus Active On-Device Intrusion Detection and Intrusion Prevention Cyber Solutions

Effective cyber security requires a selection of complimentary solutions.

- Traditional passive protection
  Firewalls and authentications are an essential part of the cyber jigsaw however they can be breached.
  Network monitoring tools monitor the network traffic down at packet level and are usually rules based on historic data, however hackers do not play by the rules and can bypass the rules algorithms.
  It should also be noted that network intrusion detection is becoming increasingly challenging, both as hacks often look and behave identically to normal users - causing high false positives, as well as requiring massive computation which is only getting harder with data consuming every greater network bandwidth.
  In addition, none of the above identify when a potential hacker has accessed the server, the access point, or the switch, and uploaded a new version of firmware to be activated in the future.
- Active intrusion detection
  Solutions such as RazorSecure are located behind the firewall and are installed as a client on the devices. Devices get hacked, not networks. The solution protects the device by using anomaly detection to identify any activity that is outside the normal including system access via the maintenance port. The system is not rules based so does not have to know the current cyber activity patterns.
- Active intrusion prevention
  Solutions that have the ability to actively protect the system in the event of a potential attack

Selection of Potential Attacks

The following table indicates the type of potential attacks that could be conducted.

Vulnerability	Impact
System access via system locker	Direct connections to internal networks and VLANs
System access via system locker	Backdoor devices on networks or engineering ports
System access via system locker	Access to USB ports on key systems

Vulnerability	Impact
Access to MAC addresses and computer names	Personally Identifiable Information leaks
GPS spoofing	GPS can be a key system for future operations.
Remote shell access	Access to system and passenger's data
Critical config file access	System can be reconfigured or key system configuration details can be leaked externally for future attacks
Unexpected authentication	System compromised
Misconfiguration	Undetected/unintentional security holes
Denial of service	Operational and passenger system unavailable
Attack on data comms server	Customer data access + defacing portal page
Attack on plane to shore wireless comms	Access to operational and possibly avionics system
DNS Spoofing	Possibility to compromise data exfiltration Possibility to compromise over the air updates
Attack into CCTV system	Access to personal data

Potential Cyber Attacks

About RazorSecure Protection

RazorSecure provides a comprehensive host based intrusion detection and intrusion prevention cyber security monitoring, detection, reporting and protection product suitable for the aviation industry helping airlines and system suppliers comply with the new cyber regulations.

The RazorSecure solution can be integrated into IFE, passenger WiFi, CCTV and electronic flight bag systems both on-board and at airport.

RazorSecure is working with GCHQ Accelerator and the National Cyber Security Centre.

Contact Robert Brown or Bob Harbon for more information.

robert@razorsecure.com

+44 7860 399068

bob@razorsecure.com

+44 7398 751447

About VT Miltope

VT Miltope are exclusively integrating the RazorSecure cyber solution within the current range of aviation wireless access points to provide airlines and system providers with the highest level of cyber protection.

Contact Markus Gilges or Jeff Drader for more information.

markus.gilges@miltope.com

+44 77937 58755

jeff.drader@miltope.com

+1 949 278-5856