Aviation Intelligence Unit
Think Paper #3 - August 2019

EUROCONTROL

Cyber Security in aviation

Being cyber secure is an illusion… let's become cyber resilient all together!

At a time when the average cost of a cyberattack is now estimated at $1 million (some recent aviation cyber incidents cost much more e.g. The fine of €204 million imposed on British Airways by the UK Information Commissioner, ASCOS being closed for 3 weeks), the objective of "just" complying with new various cyber security regulations, either aviation related, such as EC 373/2017, or not, such as GDPR or the national implementation of the EC 1148/2016 (so-called NIS Directive), is now overcome by events !

Senior management, technical staff and system designers all need to move away from the illusion that their systems/ services could manage/survive a cyber-attack because "nothing" happened in the past. They face the risk of serious business or financial consequences (though safety may not always be impaired).

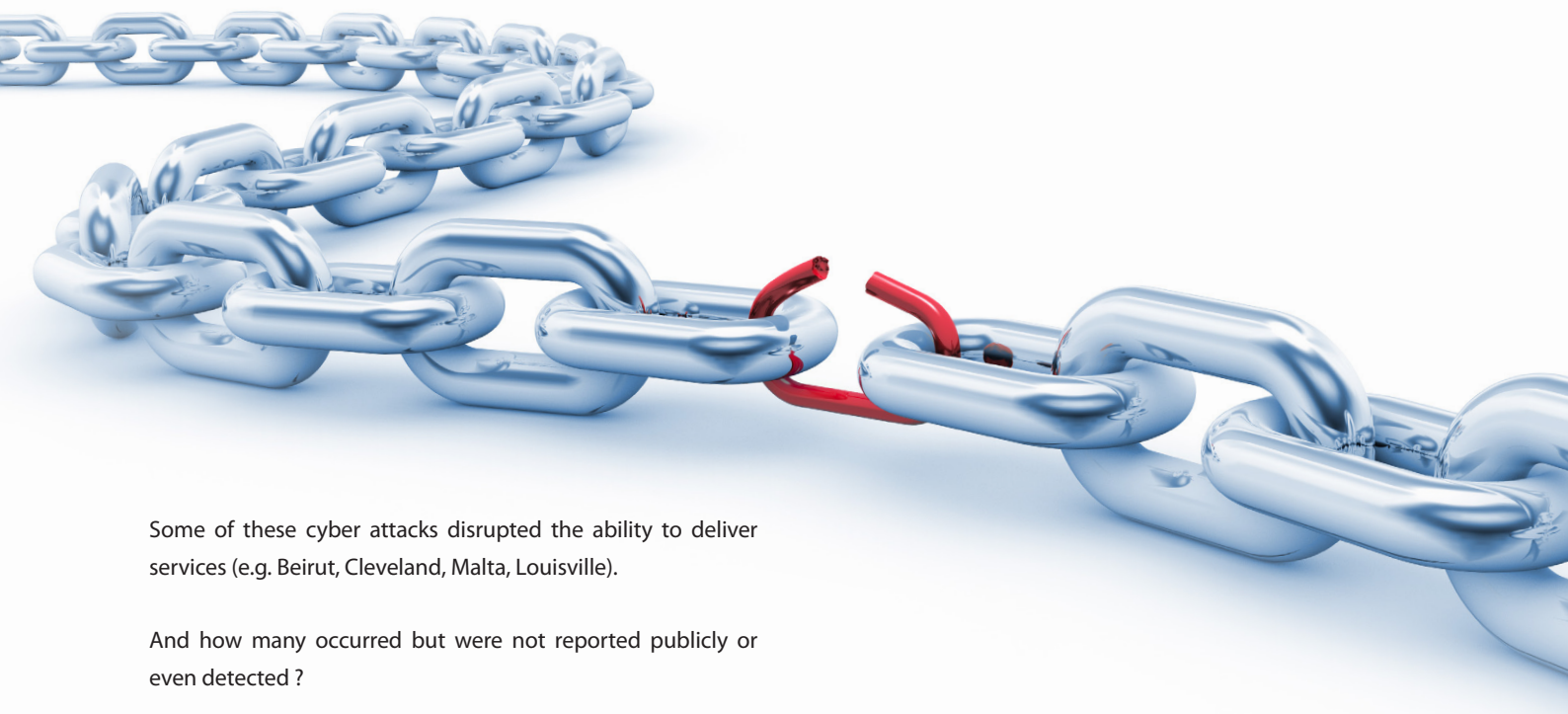
We have carried out comprehensive penetration tests / ethical hacking on many ATM systems. Let's not fool ourselves, most of current ATM systems are vulnerable.

Aviation moves towards introducing more and more digitalization thanks to new technologies and concepts using non-aviation specific means (e.g. Cloud, 5G, Internet, satellite communications and navigation). This will inevitably increase the number of aviation actors potentially impacted by a cyber attack.

The challenge now lies in making aviation systems/services progressively more and more cyber-resilient while remaining safe and cost-effective.

Risk of Cyber security evolves with a high dynamic

Figure 1:
Evolution of successful breaches of personal data (credentials, …) – time and magnitude of breaches



Some of these cyber attacks disrupted the ability to deliver services (e.g. Beirut, Cleveland, Malta, Louisville).

And how many occurred but were not reported publicly or even detected ?

The aviation eco-system has not been designed with security in mind. Aviation remains a patchwork of systems more or less loosely coupled, some being more protected than others. Conducting penetration tests on ground systems shows that the level of isolation/independence is not always as high as assumed: not a surprise to cyber-experts!

So we are living with holes and vulnerabilities in most of our systems, mostly unknown to us … but not to the hackers?!

Main threats are not under control

- **State-sponsored attacks:**
  depends upon unpredictable geo-political tensions and are too sophisticated for us to be able to pretend that they can be avoided or that we can effectively protect ourselves.

- **Cyber-crime:**
  it's an industry. Their appetite to attack aviation already exists (e.g. Fraudulent phishing emails impersonating staff to request undue payments) and may increase in an uncontrolled way. These groups are well organised and powerful. It's impossible to pretend that we can completely protect ourselves from them.

- **Hacktivism (especially for environment motivations):**
  Some groups already have targeted aviation and they will , most probably, do so more and more:

  - As aviation is a powerful means to convey messages because of its exposure to media;

  - Because of aviation's perceived negative impact on climate change.

  Those hactivists are sharp and can rely on an extended network of skilled hackers. Their motivation is their strength.

We are as strong as the weakest link

An isolationist approach cannot work in aviation because stakeholders are connected to each other. The attack may come through a stakeholder, not directly onto one's infrastructure/ systems; attacks that can impact an organisation can impact others. Attacks may also target common suppliers outside aviation, such as telecommunications or energy service providers.

The only valid strategy consists in anticipating that cyber-attacks will be successful and will negatively impact our services, systems and operations. We have to get prepared to such events in a way to reduce the magnitude and the duration of the negative impact.

One by one we are easy targets; the goal is to build a **federated** trusted cyber resilience framework.

The aviation eco-system has not been designed with security in mind

BECOME CYBER-RESILIENT … ALL TOGETHER

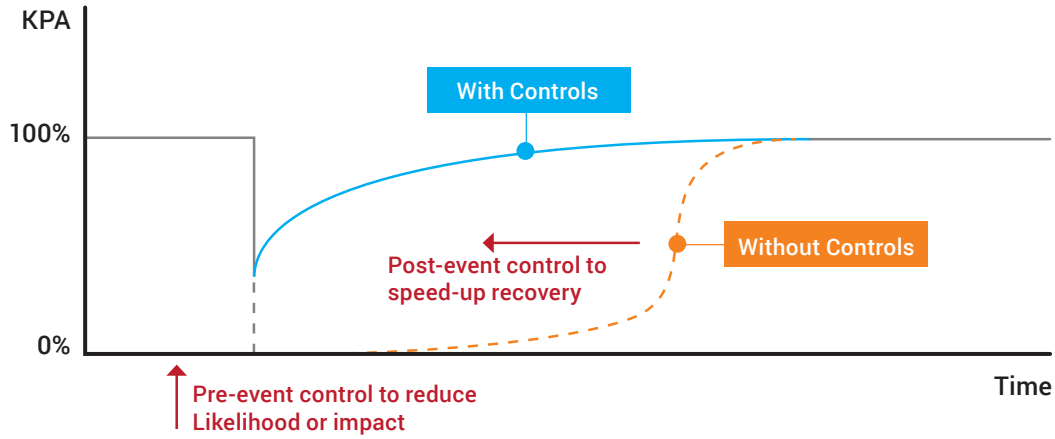


Figure 2: *Resilience*

Cyber resilience - What your organisation can do

- **Invest in Humans:**
  - Change the mindset of senior management
  - Educate, train all staff on cyber hygiene, threats
- **Adapt Processes:**
  - Implement an Information Security Management System (ISMS), aligned with other management systems. If not already done, it will be required by the EASA NPA 2019-07 "management of information security risks"
  - Conduct periodic cyber-attack exercises (table top coordination as well as technical)
- **Apply a Secure Development Lifecycle:**
  - Apply security by design to new services => ~+15% cost increase
  - Kill illusions: revisit existing safety assessments to find vulnerabilities impacting the supposed independence of safety barriers
  - Find vulnerabilities before hackers do: conduct penetration tests
  - Patch vulnerabilities while ensuring the safety of the change
  - Stop being blind: set up a SOC (security operations centre) or equivalent - the means to detect, analyse, respond and recover from cyber-attacks locally
- **Build a Trust Framework:**
  - Join in shaping a cyber regulatory framework for aviation as done by EASA through the European Strategic Coordination Platform (ESCP), promoting it at global level (ICAO)
  - Share cyber-information (de-identified is still valuable)
  - Coordinate incidents/crises at Pan-European level - Cyber is not a National only issue
  - Apply proven means that other domains have adopted for years

Let's not fool ourselves, most ATM systems are vulnerable

Cyber resilience will not make you 100% cyber-proof but will assure your business!

AND YOU CAN'T DO IT ALONE …

so let's support the establishment of a pan-European cyber resilience framework.

For more informationplease contact:

infocentre@eurocontrol.int
or
eatm-cert-group@eurocontrol.int

EUROCONTROL

SUPPORTING EUROPEAN AVIATION

www.eurocontrol.int