AIR TRANSPORT

IT REVIEW

2016

LET'S GET SMART ABOUT IDENTITY

PAGE 34

#SITAINSIGHTS

SITA
Create success. Together

DIGITAL TECHNOLOGIES ARE BRINGING MANY BENEFITS TO AIR TRAVEL, BUT THEY ALSO POSE NEW THREATS.

CYBER ATTACKS: NOT IF, BUT WHEN...

Cyber attacks targeting businesses are dramatically increasing year-on-year. Air transport has not escaped.

In June 2015, Polish airline LOT cited a cyber attack on its flight planning computers for a disruption at its Warsaw Chopin Airport hub. Two years before, a cyber attack is reported to have shut down the passport control systems in the departure terminals at Turkey's Istanbul Atatürk and Sabiha Gökçen airports causing long queues and flight delays.

There are other anecdotal reports of attacks on the industry. The Center for Internet Security (CIS) reported that 75 US airports were affected by a cyber attack in 2013, including two where the computer systems were compromised.

SILVER BULLET?

There are likely to have been many more. Few aviation businesses openly admit to being hacked in order to not erode public confidence. That makes gathering information much harder. Even industry insiders are largely working in the dark about the true scale of the problem.

What's become clear is that there is no silver bullet solution to the issue.

In fact, things are likely to get worse as the Internet of Things drives greater use of connected technologies and the proliferation of interfaces and endpoints that can be exploited.

Against this background, the panel discussion on cybersecurity at the Air Transport IT Summit 2016 was all the more timely.

COMPLEXITY

Dr Simon Moores, Security Futurist and Risk Consultant, explains: "We are starting to see such complexity of attacks – so large, so regular, and so highly scaled – that it is beyond the capabilities of human operators to handle the risk," he says.

"In 2016, it is not about if you are going to be hacked, but when," he adds.

Faye Francy, Executive Director of Aviation Information Sharing and Analysis Center (A-ISAC), gives an equally downbeat assessment. "The aviation cybersecurity honeymoon is over. We are getting attacked on a daily basis and it is unrelenting."

CALL TO ACTION

At the corporate level there are encouraging signs that businesses are ramping up their efforts to tackle the issue.

The latest Airline IT Trends Survey indicates that cybersecurity is a board level responsibility at 63% of airlines, while 72% of airlines plan major cyber- security projects over the next three years.

It's a step in the right direction, Peter Andres, VP Corporate Security, Lufthansa, believes. "We have to move the

> **"THE AVIATION CYBERSECURITY HONEYMOON IS OVER. WE ARE GETTING ATTACKED ON A DAILY BASIS AND IT IS UNRELENTING."**
>
> **FAYE FRANCY**
> **EXECUTIVE DIRECTOR, A-ISAC**

> **"WE HAVE TO MOVE THE DISCUSSION ON CYBERSECURITY FROM THE EXPERT LEVEL TO THE CORPORATE LEVEL."**
>
> **PETER ANDRES**
> **VP CORPORATE SECURITY, LUFTHANSA**

discussion on cybersecurity from the expert level to the corporate level."

The German flag carrier has been doing this since 2013. It defined five levels of activities as Andres explains.

"First, locate cybersecurity and find a joint perspective between IT and security.

"Second, increase cooperation with stakeholders in industry.

"Third, perform risk analysis for the business divisions – we identified 20 business areas critical to Lufthansa's performance. Four, upgrade IT. And five, perform a process analysis exercise and feedback into the organization."

JOURNEY OF LEARNING

But Francy believes the rapidly emerging cyber threat landscape is also a clarion call to get organized and coordinate efforts to tackle the issue at the community level.

"There is a need for us to come together as an industry and to recognize that there are potential vulnerabilities as we interconnect everything," she says.

Working hard in this area is Francy's (A-ISAC. It's a non-profit making organization for sharing security information in the industry.

WHAT IS A-ISAC?

The Aviation Information Sharing and Analysis Center (A-ISAC) is a non-profit making member-driven organization for sharing security information in the aviation sector.

It was formed in September 2014 by seven major aviation companies. Today it has 22 members from across the aviation sector.

The A-ISAC gathers threat, vulnerability and risk information about security risks facing the aviation sector around the world. Sources of information include members, government agencies, academic sources, open source and other trusted sources.

Its goal is to share the information in a timely, actionable way, as well as build up a body of subject matter experts that can share mitigation techniques.

More information on A-ISAC can be found at **www.a-isac.com**

> **"CYBER SECURITY THREATS ARE GROWING FASTER THAN CYBER SECURITY MITIGATION MEASURES."**
>
> **DOMINIC NESSI**
> **AIRPORT TECHNOLOGY CONSULTANT AND MEMBER OF THE ACI WORLD TECHNOLOGY STEERING GROUP**

OPINION

COULD ARTIFICIAL INTELLIGENCE BE THE ANSWER?

By Dr Simon Moores, Security Futurist and Risk Consultant

If you think about some of the numbers around cybersecurity, it becomes quite scary:

- 1.2 million polymorphic viral threats being created each day.
- Cyber criminals using bot armies with a quarter of a billion bot attacks on a daily basis.
- 264 million attacks by botnets alone in the first quarter of 2016. That's about 35 per second.
- More than half a billion records reportedly stolen last year, suggesting that large businesses will suffer an attack, on average, around three times each and every year.

One area that is getting a lot of interest from companies, such as IBM and Google and others, is Artificial Intelligence (AI). What we are starting to see is the evolution of something called deep learning and machine learning which we can start to think of as a solution to be used in the information security space.

See full online article at:
www.sita.aero/air-transport-it-review

> **"IN 2016, IT IS NOT ABOUT IF YOU ARE GOING TO BE HACKED, BUT WHEN."**
>
> **DR SIMON MOORES**
> **SECURITY FUTURIST AND RISK CONSULTANT**

"Our goal is about sharing timely, actionable, relevant information and analysis on threats and vulnerabilities to aviation," she explains (see 'What is A-ISAC?').

Francy sees it as "a journey of learning". She says: "We must look at how to prevent the attack, but in the event that we don't, we must be able to identify and detect the threat, mitigate it and then build resiliency into what we do."

INITIATIVES

There are also other industry initiatives ongoing.

Just last year, Airports Council International (ACI) set up a cybersecurity task force to develop a community approach for airports.

Meanwhile, IATA is trying to bolster the cyber defenses of airlines with a security tool kit that includes training videos, a risk analysis tool and other resources.

WEAKEST LINK

The importance of collaboration was echoed by Dominic Nessi, Airport Cybersecurity Consultant working with Burns Engineering.

"This is an industry-wide problem. A common approach is critical. We need to start with education and information sharing, proceed to mitigation and defense techniques and work as a community."

Nessi is particularly concerned that many airports are much less resourced than their larger partners in the industry and this will impact their ability to tackle cyber threats.

"Cyber security threats are growing faster than cyber security mitigation measures. I don't worry about large airports, but I do for all of those medium-sized and smaller airports," he says.

"If you have a breach anywhere, it can affect our entire system. How do we assist airports in emerging economies?" he continues.

"Many airport managers, if they don't see this as a threat they are not providing funding." See 'The Airport Cybersecurity Challenge'.

SKILLS AND BUDGETS

Thomas Gourgeon, Head of International Operations, Orange Cyberdefense takes up the resourcing issue.

"Security is a field where there is an immense skills shortage and of course security budgets are not unlimited," he says. "You need access to IT experts, security analysts, security researchers."

Gourgeon believes it's a lot of diverse skills for the IT department to master and companies would be better served partnering with experts.

"If I take the example of Orange Cyberdefense it's a group of 800 people dedicated to security so it helps us attract, it helps us retain, the best people," he says.

HEAR OUR EXPERTS

Search the **SITA Online YouTube channel** to hear expert commentary on **'Cybersecurity - tackling the threat'** from:

Faye Francy, Executive Director, A-ISAC

Dr Simon Moores, Security Futurist and Risk Consultant

Dominic Nessi, Airport Technology Consultant & ACI World Technology Steering Group

Thomas Gourgeon, Head of International Operations, Orange Cyberdefense

OPINION

A TIERED APPROACH IS THE BEST DEFENSE

By Thomas Gourgeon, Head of International Operations, Orange Cyberdefense

To really tackle the whole cyber threat landscape needs a specific approach. What I call a four tier approach.

- The **first layer** is the basics. It's important to get the basics right and by this I mean user awareness.
- The **second layer** is reactive. It's about firewalls, it's about proxies, it's about identity and access management technologies that have been out there for the last 10 years.
- The **third layer** is proactive. You have to go beyond reactive protection and look at what's actually happening within your infrastructure.
- The **top layer** is predictive. This is where you need threat intelligence and R&D.

I think that there's a lot of learning to do and a lot of expertise needed if you want to do it right. This is why you may want to consider relying on partners rather than going down the full Do-It-Yourself route.

See full online article at:
www.sita.aero/air-transport-it-review

"Another thing is that, as a network operator, we are in the middle between the attackers and their targets. For example, we are able to listen to what's going on and pick up the signals for Denial of Service (DoS) attacks.

"It means we can define countermeasures 30 minutes in advance of the website attack," he continues.

GOVERNMENT LEAD

Nessi believes the industry cannot work in isolation if it's to deliver a concerted response to the issue. "The airport community needs to work with government," he emphasizes.

It's a view endorsed by airlines, with IATA saying cybersecurity can best be managed through stronger collaboration between the governments and key industry stakeholders.

There are signs this is starting to happen. In the US, the Federal Aviation Administration (FAA) has been tasked by the government with developing regulations on cybersecurity, including mandatory reporting of incidents.

At the global level, a more coordinated government approach could get a kick start in 2017 when aviation associations, such as IATA, present a declaration on cyber security to the United Nations' aviation safety arm.

COLLABORATION

With the lack of international oversight on cybersecurity, who should be responsible for coordinating the efforts? The answer is not so simple. "There is no one owner, no one regulatory body," points out Francy. She believes the

OPINION

THE AIRPORT CYBERSECURITY CHALLENGE

By Dominic Nessi, Airport Technology Consultant and member of the ACI World Technology Steering Group

Despite being one of a country's most important and critical infrastructures, airports are not well-suited to address the challenges of an insecure cyber world.

- First, airports traditionally attempt to keep operating costs as low as possible so that their airlines can operate in the most cost effective manner, and effective cybersecurity measures do have a cost.
- Second, airports come in a variety of sizes and all but the world's largest airports tend to have a very small information technology staff.
- Finally, the cyber risk to an airport is generally not well known or understood at the airport management level and, as a result, may not always get the attention that it deserves.

Led by ACI World's **Cybersecurity Task Force**, ACI is currently developing an **IT Cybersecurity Benchmark Tool** that will allow airports around the globe to compare their current cybersecurity efforts with the ISO standards 27001 – 27003.

In addition to the Benchmark tool, **ACI's Cybersecurity Task Force** offers a **Ten-Point Approach** to the airport community to increase its cyber-awarenes, as articulated in the full online article.

See full online article at:
www.sita.aero/air-transport-it-review

A-ISAC is currently the best way for the industry to unite against common threats.

There is also the issue of trust. "Companies are resistant to publicly or directly sharing their threat intelligence information. They don't want to see it in the media," she says, adding that "In A-ISAC we anonymize the information that members don't want to share directly."

Nonetheless, there's a strong consensus that to assemble a well-orchestrated cybersecurity risk and mitigation strategy, the industry must find a way to come together if it's to move in the right direction. SITA is playing its part working with its members and other industry partners to support this goal.

In the meantime, Moores believes the battle between cyber attackers and IT security specialists will only escalate. "It is an arms race", he declares. ■