AAAE DELIVERS FOR AIRPORT EXECUTIVES

Airport MAGAZINE

www.airportmagazine.net | August/September 2016

SECURITY

Trusted Agent: The Airport's First Line of Security

Biometrics: A Technology in Every Airport's Future

The Cybersecurity Risk: What does it Mean for Airports

THE CYBERSECURITY RISK: What Does it Mean for Airports?

BY FAYE FRANCY

Each year, the global air transportation system carries nearly 3 billion passengers and close to 50 million tons of freight. It supports nearly 63 million jobs and $2.7 trillion in global GDP; one third of all global trade (by value) is sent by air.

There can be no doubt that aviation is one of the largest drivers of our global economy. As such, it represents a major critical infrastructure with assets and systems essential to our way of life.

In the past, the businesses that make up the aviation industry operated as isolated systems. Today, however, the advancement of technology has enabled the creation of interconnected networks that provide economic value and operational efficiencies beyond imagination just a few decades ago.

Certainly, this connectivity has provided immeasurable benefits. Just as we examine the benefits, however, we also must explore the risks and emerging threats. Our interconnectivity has introduced a new avenue for threat actors seeking to disrupt and cause harm for personal, political, religious or other reasons. Even as the news is filled with reports of physical threats and attacks at airports around the world, cybersecurity risks and potential attacks loom large for airports, and the entire aviation industry.

Cyber incidents can have devastating consequences on both physical and networked infrastructures. As early as 1998, the U.S. federal government recognized the potential for major critical infrastructures to come under attack from cyber threat actors. As a result, U.S. Presidential Decision Directive/NSC-63 (PDD-63) was signed, asking each critical infrastructure sector to establish sector-specific information sharing organizations in order to maintain open channels of communication about current threats and collaborate to forestall potentially devastating attacks. In 2012, the Aviation Sector Coordinating Council formed a working group that identified the global need for an organization focused on improving coordination and protection response in the aviation sector. In 2014, seven global aviation companies joined together to form and incorporate the Aviation Information Sharing and Analysis Center (A-ISAC).

A nonprofit 501(6)(c) membership organization, the A-ISAC welcomes private sector firms that do business principally in the aviation sector of the economy. The organization engages with other private sector sharing organizations facing the

same cyber challenges. Additionally, the A-ISAC works closely with government partners to share and receive actionable intelligence. In the U.S., the A-ISAC has established close working relationships with DHS, TSA, FAA, FBI and the Office of the Director of National Intelligence, and we are now engaging with European and other international government agencies.

Through its membership and trusted partner relationships, the A-ISAC enhances the ability of the aviation sector to prepare for and respond to security threats, vulnerabilities and incidents, and to reduce the risks and costs associated with operational disruptions due to nefarious security events.

The ability to effectively provide threat intelligence to protect the aviation sector truly has become an operational requirement for global air transportation stakeholders, airports among them. Airports are critical to the global air transportation system, and each airport has a unique responsibility to ensure that every passenger, piece of freight, or commercial product is transported safely to its destination, with minimal disruption and risk as possible.

Airports are akin to small cities, with people, goods and services flowing through the infrastructure daily. Airports are the hubs for aviation — a place where our global air transportation system connects with other modes of transportation. And in today's world, airport users demand connectivity while spending time in the airport environs. Almost every passenger traveling through an airport has some sort of mobile device that he/she wants to use — all representing possible threats or inroads to airport infrastructure. This risk highlights not only traditional IT infrastructure challenges but also the added challenge of the use of the airport for airlines to connect and service their aircraft. The airplane is a global, mobile industrial control system; understanding this risk requires additional skill sets. It is imperative that airport directors take the consequences of cyber risk very seriously.

The recent terrorist attacks in both Brussels and Istanbul have demonstrated the devastating human and economic impact caused by malaligned threat actors. While these bombings are kinetic in nature and are considered physical attacks, it is important to realize that operatives are beginning to integrate cyber methodologies to seek key information about their intended targets and victims as part of their planning activities. Thankfully, the ability of terror groups to use cyber tactics is still in its infancy. Right now, this is good news for airports, as it provides a window to implement key strategies and systems, design response and recovery plans, educate staff, and prepare for the day when terrorist cells are able to embrace cyber as a viable weapon in their arsenal.

Benefits of Information Sharing

The benefits of information sharing in this new digital era far outweigh the potential vulnerabilities. It certainly goes against traditional business principles to share information with other companies and organizations considered to be competitors, but it is being done and with impressive results. The alternative of not having such information available in a timely manner brings dire consequences. Yet, despite its importance, information sharing across companies remains a challenge for most organizations. Know that the bad actors are sharing information far better and much quicker than the good guys — this is why their tactics, techniques, and procedures are being reused — and delivering results. We must incorporate sharing as a key security control in thwarting this most ubiquitous threat.

> The ability to effectively provide threat intelligence to protect the aviation sector has truly become an operational requirement for global air transportation stakeholders, airports among them.

Two recent examples highlight the value that information sharing across organizations and trusted partners brings to the ongoing battle against cyber attacks.

In 2013, a trusted partner of the A-ISAC identified an Advanced Persistent Threat (APT) attack campaign targeting airports across the United States. Airports were notified, and one major international airport requested assistance to identify the scope of the incident. The results of the analysis identified that a user on the airport network had clicked on a link in a phishing email; that link downloaded a malicious executable. The trusted partner and the airport worked together to create and implement a mitigation plan that included specific recommendations and actions. This mitigation plan was shared across trusted partners, enabling other aviation sector businesses to shore up their systems and prevent similar infiltration.

More recently, in early 2016, a third-party vendor identified a viable threat against a small, regional airport in North America. Although the vendor tried to contact the airport directly, the airport did not believe the outreach was legitimate and essentially ignored the warning. The A-ISAC became involved and was able to facilitate a successful conversation among the third-party vendor, members of the A-ISAC community, and, importantly, the airport. The airport was made aware of the risk and, by working collaboratively with both the A-ISAC and its member community, was able to take appropriate mitigation steps.

Recommendations

Fighting the cybersecurity threat is truly a global "team sport" for the aviation industry, and airports are key players on that team. Implementing cybersecurity best practices and joining information sharing organizations is key to building resiliency into your infrastructure.

Cyber is not solely an IT issue, it is a business issue — ensure it is being addressed at the appropriate levels. No airport will ever be 100 percent secure from cyber attacks, but there are some best practice offensive tactics airports can — and should — begin to implement. Cybersecurity is now a cost of doing business.

Managing risk is a key element of cybersecurity protection and building resiliency is essential. It is not a question of if an attack will happen, it is a question of when. Institutionalizing an incident response and management approach is a key step toward risk mitigation. It is essential in improving threat

response and recovery to have a solid incident response plan that is exercised routinely. Additional capabilities include threat modeling, vulnerability assessment and forensic analytic capabilities.

Last, creating a "culture of security" is critical. Building blocks include embedded network security requirements, training and education, and expanding focus beyond safety to include security and resiliency. Training and awareness are critical elements in any strategy, as are exercises to ensure you know what to do when the attack happens. Working with trusted aviation partners will help in the global fight.

While there is much to be done at the operational and infrastructure level, it is also the responsibility of individuals working within the organization. As in the 2013 APT attack mentioned above, employees unknowingly can open the door for those seeking to do harm. Email remains a primary method for threat actors to infiltrate a system. Even though organizations have installed filtering capabilities, phishing emails still may get through. Hackers are "spoofing" email sender addresses from major companies and services, tricking recipients into thinking the malicious message is from a known and/or trusted provider.

Encourage employees to "Think before you click" and trust their judgment regarding emails that look strange or suspicious. Examine email addresses and notify the IT security team before opening. It is incredible how many infiltration attempts have been stopped as a result of recipients paying attention.

In addition to the high-level recommendations provided here, The Transportation Research Board of the National Academies has published ACRP Report 140: Guidebook on Best Practices for Airport Cybersecurity. Written by Randall J. Murphy and Michael Sukkarieh of Grafton Technologies Inc., and John Haass and Paul Hriljac of SoftKrypt, this comprehensive report provides airports with a great starting point to identify the primary activities and key roles and responsibilities for a cybersecurity program. It provides guidance on implementing countermeasures, developing a cybersecurity program, and detecting, responding to, and recovering from attacks. It is available online at **http://onlinepubs.trb.org/onlinepubs/acrp/acrp_rpt_140.pd**f and is an excellent resource.

Cyber Threat Is Real

Vigilance is key and everyone plays a part in protecting the aviation sector. Airports and their employees have the "inside" perspective. If something seems "off," it very well may be. The A-ISAC mantra is, "If you see something, say something." Don't wait for an incident to try to identify the appropriate cyber response team. It could very well be too late.

The cyber threat is real, and it is not going away any time soon. Just as threat actors work to share information and tactics, we, too, must work as one to share information, risk mitigation techniques, threats and challenges, and more. One company's detection of a potential attack may mean another company's prevention of a devastating security breach.

For more information on Aviation ISAC, visit www.a-isac.com or email **membership@a-isac.com.**

Faye Francy is executive director, Aviation ISAC. She may be reached at ffrancy@a-isac.com.

RICHARD CLARKE'S Top 10 Cybersecurity Principles

1. Don't be in denial
2. Don't underestimate the problem
3. Don't be hostile to the government
4. Don't make it an issue buried in the bureaucracy, not just a CIO issue
5. Organize ISACs, sponsor R&D work
6. Think holistically
7. Don't attempt to defend the entire network
8. Identify the crown jewels
9. Look at worse case scenarios
10. Have an industry strategy

Source: *Richard A. Clarke TOP 10 LIST*, Chairman and CEO, Good Harbor Risk Management, LLC, AIAA Conference, August 2013