In Part 3 of our Aviation perspectives series on cybersecurity in the airline industry, we look at the importance of early detection—the discovery of a threat or attack as close to the moment it actually begins. Because while prevention is the best defense, not all attacks can be prevented.

At the recent Air Transport IT Summit, experts agreed that “in 2016 it’s not about if you’re going to be hacked, it’s when.”¹ And when the inevitable occurs, it’s critical to have defenses in place that can minimize damage to the organization.

When dealing with a cyber incident, organizations often discover that there were signs of an intrusion long before the breach was identified. In our experience, advanced threat actors often maintain remote access to the target environment for 6-18 months before being detected. During this time, an attacker has the opportunity to identify critical systems, locate valuable data, and execute the most devastating attacks. Early detection, along with a clearly defined set of operational processes to quickly address an attack, is vital to reducing the consequences. This is true for all industries, including the airlines.

The objectives of today’s advanced cyber threats are typically to steal desired data and maintain access to the environment for as long as possible. Over the past decade, in all industry sectors, cyber intrusion activity targeting multinational companies has increased significantly. Any company with proprietary data perceived to be of economic value—or involved with national security and critical infrastructure, such as aviation—has increased from a potential to a likely target.

When compromised organizations conduct incident post-mortem analyses, they usually discover that their monitoring processes and tools are lacking. They may not have a holistic view of systems and data across the enterprise and they may not include needed alerts, rules, and workflow to detect or communicate threat scenarios.

In fact, we see that many current tools only perform basic pattern matching and counting and fail to correlate data across multiple systems and between seemingly disconnected events.

**Part of the challenge of detecting security breaches** is keeping up with the constantly evolving set of threat actors, targets, and vectors. Detection protocols have to be one step ahead of the latest hacking techniques. Another problem is that while external threats get more play in news headlines, insider threats can be much more difficult to diagnose and costly to remediate.

Companies also face a financial challenge: When it comes to cyber strategy, it is often more difficult to obtain funding for detection efforts than for prevention. Preventative measures, such as encryption and access control, are often tangible and, as a result, easier for management and employees to understand and support.

Detection, on the other hand, is a moving target with generally unknown actors, uncertain penetrations, and unpredictable timing. Since attacks are so varied, it can be hard to build a leading-edge detection system. Airlines face an additional burden in that they have extensive third party networks. And for all industries there is little concrete regulatory guidance other than the International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST).
**Include detection in cyber programs**

The leading airlines that include detection as part of their cyber programs have built comprehensive coverage of their network, data, and endpoints. They’re able to react so quickly to attacks that response times are virtually instantaneous. This ability to move decisively and swiftly not just limits losses, but also prevents the intruder from temporarily pausing the attack and hiding elsewhere in the enterprise’s networks only to attack in a different fashion at a later date.

<table>
<thead>
<tr>
<th>Develop quantified and measurable baselines</th>
<th>Create current education and training</th>
<th>Scope and prioritize assets</th>
<th>Collaborate internally</th>
<th>Acquire broad expertise</th>
</tr>
</thead>
<tbody>
<tr>
<td>By establishing baselines for data transmissions, volumes, and times, an airline can determine when an event has occurred that is outside the norm.</td>
<td>Employees need to be taught to recognize suspicious behaviors and how to deal with them.</td>
<td>It’s important to prioritize assets to focus more detection capability on the “crown jewels,” such as personal passenger data (including credit card data) and operational systems.</td>
<td>Airlines have to build collaborative systems within their own organizations. This requires breaking down walls with cross-functional operating procedures and creating incident response processes that are embedded into business processes. So when a breach is detected, relevant groups throughout the airline are alerted and can react in a more timely and unified way. There should also be formal processes for actively sharing new threat intelligence, to allow for more effective monitoring mechanisms going forward.</td>
<td>Leave “profiling” to the experts, those who can interpret activity reports and understand anomalies to recognize false positives and signs of a real attack. These experts have intimate knowledge of enterprise networks, endpoints, domains, and operations that is paired with industry-wide experience and knowledge of evolving threat actors, techniques, and tools.</td>
</tr>
</tbody>
</table>
Investments are made in state-of-the-art tools, which are deployed and configured to each enterprise’s specific operating circumstances. This includes cloud-based threat detection that is closer to the endpoints where intrusions frequently begin. Often, how well tools are configured to meet the needs of the specific organizations is more important than the technologies themselves.

Clearly defined protocols reduce the time from incident to detection to response. Protocols include sensitivity and analytical capability that can discern false positives driven by external or internal events unrelated to an intrusion.

Defense tools must stay ahead of threats. Signature-based defense tends to be static (e.g., signatures become obsolete, security protocols and tools can be reverse-engineered). One way to achieve greater flexibility and timeliness is to leverage the capabilities and infrastructure of subscription-based services that utilize the cloud. These services provide real-time updates that aggregate information and keep defenses fresh and dynamic.

Initially, this requires analysis of what’s missing and investment to fill the gaps. Second, it requires expanding coverage of monitoring solutions to bridge the large, operational on-premise systems (e.g., HR) with new cloud systems and other technologies around the airline (e.g., IFEC). Lastly, it requires investing in an operations center with dedicated perpetual cyber capability. This allows monitoring of the physical environment, external service providers, and personnel activity. With the creation of a centralized department, detection processes can be tested and continually improved.

Collaboration of threat intelligence among airlines is an important defense to early detection and helps thwart industry threat actors. This can be done through tools that provide the ability to share identified threats with other subscribers and, in some cases, automatically interact and collaborate on detecting and managing related threats. As with physical security today, collaboration among airlines, airports, and other key stakeholders would serve to share attack/ intrusion specifics and warn airlines about current and future threats.

While cyber detection has to be tailored to meet the specific needs of each airline, these tools can not simply log and aggregate data points—they have to intelligently correlate the data to identify an intrusion. In addition, next generation cyber security defense programs include other essential capabilities such as those discussed below:
Companies in the aviation industry face yet another challenge. A key trend is increasing interconnectedness, whether it’s between aircraft and ground control stations, airlines, airports and other aviation stakeholders, or between dispersed field-deployed assets. This same interconnectedness that provides operational efficiencies simultaneously introduces further risk to commercial passenger airlines. From billing and reservation systems to aircraft engine telemetry, aviation companies have broad networks that not only provide multiple high-value targets for attackers, but because of their interconnections open up multiple avenues of penetration into an airline’s core systems. A recent example of the danger inherent in interconnections with third parties occurred in the attack on an organization’s air-conditioning vendor, which then allowed hackers to penetrate the corporate network. While there’s no going back on interconnectedness—it is a factor in today’s world—every airline has to address the risk of third-party networking and the potential weakness of points of intersection.

Compounding the challenge of implementing and maintaining an effective cyber detection program are the many seismic changes in the airline industry in recent years that add to complexity. Below are some changes we’ve seen that alter the way airlines operate and make it more difficult to detect cyber threats:

- growth in the volume and types of data created by new-model airframes, engines, and components
- increased focus on capturing, mining, and using passenger shopping and travel preferences and behaviors
- proliferation of increasingly advanced and interconnected assets among aircraft, airports, airline network operations and dispatch, and other stakeholders in the travel ecosystem
- increased dispersion of data collection points, geographically and physically
- increase in the number of vendors that tap into and use airline data to improve operations, passenger management, and other core airline functions
- reliance on potentially insecure legacy applications and platforms that support core aircraft operational activity

Detecting cyber: The unique complexity of an airline ecosystem increases the importance of an interconnected strategy.
Since airlines can pay a particularly heavy toll for not having effective cyber detection tools, they’ve become much more proactive in developing tools as part of their cyber programs. According to the latest Airline IT Trends Survey from SITA\(^2\), 91 percent of airlines are planning to invest in cyber programs over the next three years, up from 47 percent in 2013. The study also shows a large increase in the number of airlines that think they are prepared for the common types of cyber threats: 48 percent compared with 17 percent three years ago.

To create an effective and comprehensive detection program, airlines will need to tackle special challenges. Airlines operate in a dispersed model that requires their assets, people, processes, and technology to span the reach of their network. In addition to this, they must consider other stakeholders and third parties they rely on that have unique access to their assets and systems. These include aircraft, engine and component OEMs; partner airlines; global distribution systems and travel agencies; and airport operators and air traffic control systems. With increased interconnectivity both within airlines and between airlines and other aviation industry stakeholders, the importance of a good detection program has become increasingly important. After all, an airline’s overall cybersecurity strength is only as good as the weakest link in the chain.

In the next part of this airline cybersecurity series

We’ll look at ways airlines can react effectively to an attack. With so much at stake, airlines must continuously learn from cyber incidents how to minimize damage to their customers, company reputation, finances, and operations. Cyber attacks are a matter of “when,” not “if.” Decisive action and a robust process can help ensure that an airline emerges from each attack stronger and more capable to meet and deflect the next one.

---

Contacts

To have a deeper conversation about the subjects discussed in this report, please contact the following:

PwC airline specialists:

Jonathan Kletzel
US Transportation & Logistics Leader
+1 (312) 298 6869
jonathan.kletzel@pwc.com

Alexander T. Stillman
US Transportation & Logistics Director
+1 (202) 487 8086
alexander.t.stillman@pwc.com

Rajeet Mohan
US Transportation & Logistics Director
+1 (305) 375 6239
rajeet.mohan@pwc.com

Bryan Terry
US Transportation & Logistics Managing Director
+1 (678) 419 1540
bryan.terry@pwc.com

Richard Wysong
US Transportation & Logistics Director
+1 (415) 498 5353
richard.wysong@pwc.com

PwC cybersecurity specialists:

Charles Beard
US Advisory Principal, Forensic Services
+1 (703) 918 3318
charles.e.beard@pwc.com

Rik Boren
US Advisory Partner, Cybersecurity and Privacy
+1 (314) 206 8899
rik.boren@pwc.com

Mickey Roach
US Advisory Partner, Cybersecurity and Privacy
+1 (214) 756 1635
mickey.roach@pwc.com

Mir Kashifuddin
US Advisory Director, Cybersecurity and Privacy
+1 (214) 754 4537
mir.kashifuddin@pwc.com

Darren Orf
US Advisory Director, Cybersecurity and Privacy
+1 (312) 298 5072
darren.c.orf@pwc.com

Vincent Scott
US Advisory Manager, Cybersecurity and Privacy
+1 (513) 768 6397
vincent.h.scott@pwc.com

Editorial contributor

Gloria Gerstein

For general inquiries, contact

Diana Garsia
US Transportation & Logistics Marketing Senior Manager
+1 (973) 236 7264
diana.t.garsia@pwc.com

Visit us at pwc.com/us/airlines
Follow us on Twitter @PwC_Aviation
Read our blogs: usblogs.pwc.com/industrialinsights/category/airlines