AVIATION SECURITY INTERNATIONAL

www.asi-mag.com

THE GLOBAL JOURNAL OF AIRPORT & AIRLINE SECURITY

Beijing Convention & Protocol:
responding to future threats

ALSO:
CYBER SECURITY
CONTROL MECHANISMS
ICAO CONVENTIONS
UNRULY PASSENGER RESTRAINT

PRINCIPAL MEDIA SPONSOR TO:
AVSEC World 2010

OCTOBER 2010 VOLUME 16 ISSUE 5

AVSEC IN THE SOUTH PACIFIC
SEE PAGE 20

COCKPIT LASER ILLUMINATION
SEE PAGE 26

CYBER SECURITY:
THE HACKING THREAT

Online check-in is available in most airports; self baggage check is becoming a reality; baggage reconciliation systems are automated; computers help air traffic control coordinate the path of airplanes. The age of technology has most definitely arrived. It has brought with it a whole new breed of terrorists: cyber terrorists. Stacy A. Shannon looks at how it is changing the role of aviation security around the world.

As technology becomes more and more commonplace and relied upon, the consequences of its failure have become even greater, according to Karl Rauscher, chief technology officer and distinguished fellow of the East West Institute, an international think tank with offices in the United States, Belgium and Russia. "The bigger picture is that we're depending on the technology more and more," he said. "Dependence is growing every year." Jón Kristinn Ragnarsson, who recently received his master's degree in international relations from the University of Iceland and has studied cyber security in Iceland, agreed with Rauscher. He said with technology advancing rapidly and the industry depending heavily upon it, serious security infractions could have already occurred. "I would not be surprised if the possibility to board a plane undetected was already at the disposal of criminals," he said. "It could, of course, even have happened, but we just don't know about it. It would be in the interest of the government [and] airlines that the general public not know about things like that. The extent of these crimes has probably not yet been realised."

Dr. Rex Hughes, associate fellow of cyber security at Chatham House, a think tank in the United Kingdom, said while terrorists may be able to do things such as a board a plane anonymously or even check bags undetected, major airport operations would most likely be their prime target. While he doesn't know of any instances where air traffic control has been penetrated, he said mechanical failures causing a similar situation have shown how vulnerable those systems really are. "It doesn't take much for either a technical flaw or the equivalent of a cyber attack to cause significant damage, if not loss of life," Hughes said. "Could a cyber attack disable parts of the aircraft control system? Sure, it's definitely possible, but the likelihood at this time is pretty low. The risk may increase as the technology itself evolves."

The advancements in technology have also decreased opportunities for behavioural analysis, according to Norman Shanks, visiting professor in aviation security for Coventry University in the United Kingdom and principle partner of NSAI, his international group of consultants for aviation security and business management. "One of the basic but key elements of security used to be the face-to-face interaction between the airline check-in agent and the passenger," said the 42-year veteran of the aviation security industry. "However, the increasing introduction of both self check-in and bag check-in has removed all human contact at the check-in stage and, while apparently improving customer service, it has paradoxically created an exploitable gap in the overall security package." Desk agents trained in behavioural analysis or relying on their own intuition are no longer the forefront in identifying potential threats to the airport and flights.

The Technical Side

With such a strong reliance on technology, protecting important systems such as air traffic control and baggage reconciliation is vital. Shanks said the responsibility for protecting such systems starts with IT managers but overlaps with security professionals as well. "It should be expected that the IT managers are aware of and have countermeasures to address such risks," he said. However, he added, security managers are also responsible for coordinating with IT managers to ensure that cyber security is incorporated into the overall airline security programme to ensure that networks remain secure.

Hughes pointed out that one of the greatest battles is getting the funding to keep up with technology. For example, many airlines, particularly in the United States, are using legacy systems meaning that the systems have been around for years and the vulnerabilities are known. Or they are using off-the-shelf products or mass manufactured and retailed products which also have known vulnerabilities. These systems and products can leave airlines open to hackers, according to Hughes. "The right approach is to think about where companies can improve their existing platforms and make them more secure," he said. "The physical and virtual are now one. Developing innovative solutions is going to require both physical and virtual security experts to sit down at the same table and come up with a holistic solution to these problems."

One solution to software and hardware vulnerability comes into play before the systems are even installed, according to Rauscher. He said from a security standpoint, airlines and airports must assess the integrity of where their software and hardware are being manufactured. Many times these items are developed in geographic areas of less stability and so are at greater risk for compromising information to fall into the hands of terrorists. "We need more policy work in that area," Rauscher said. "Every sector is dependent on outsourced software and hardware." Along those lines, he said airport technology should be built with hardware and software from different vendors as well. That way if one system fails, all operations aren't shut down.

Keeping vital operations closed off from the internet is also important. Tammy L. Jones, from the U.S Federal Aviation Administration (FAA), said this comes into play especially for air traffic control systems. "The FAA's air traffic control system is a secure internal network in which no critical systems access the internet," she said. "All FAA networks are extensively monitored using intrusion detection sensors for signs of suspected adverse cyber activity."

Some companies specialise in products designed to identify when such threats are taking place on a network. AirTight Networks CEO David King said his company specialises in wireless network security. He pointed out that lots of airports utilise WiFi as part of their infrastructure. Hackers can attach devices to such networks if they aren't well secured. "Airports are among the type of enterprises that should take the threat more seriously than average," he said. His company partnered with Gartner Mobile and studied 14 airports throughout the United States, Canada and Asia. They found that nearly 80 percent were using unsecured encryption and determined there was a high probability that some of those unsecured networks were being used for critical airport operations. AirTight Networks makes a Wireless Intrusion Prevention System (WIPS) that can classify connections being made in and around airports, block threats and physically locate where the intrusion is happening. "The last thing you want is for an airport to be shut down," King said.

Another component to consider when assessing cyber security is a plan of action for what to do if an attack occurs, according to Dr. Vladimir Golubev, founder and director of the Computer Crime Research Centre in the Ukraine. "First of all, these risks cannot be underestimated," he said. "And there should be a regulation by security policy designed to minimize damage in case of hacker attacks."

The Human Component

Employing good practices to protect technology and even additional technology to protect automated systems is only part of the battle against cyber terrorism. Humans most definitely come into play as well. Though systems are automated, most still have human operators behind them who are fallible.

Rauscher said even the best employees have basic vulnerabilities inherent to all humans. They get tired, can be deceived, can have a cognitive challenge, can have divided loyalties and can even just make mistakes such as hitting the wrong key on the keyboard. "Those intrinsic vulnerabilities always exist," he said. "You can't ever take them out of anybody. One of the first steps is realising how truly vulnerable any human being is. The second step is to systematically and thoroughly address as best you can with practices by implementing countermeasures to address intrinsic vulnerabilities in a systematic way." Countermeasures

"...security managers are also responsible for coordinating with IT managers to ensure that cyber security is incorporated into the overall airline security programme..."

can include things like making sure employees are getting enough rest, adequately compensating them so they aren't tempted to compromise systems for extra money and setting up checks and balances so that one person or group doesn't have too much influence.

Another countermeasure for identifying divided loyalties is background checks. Alain Establier, managing director of Airport Security Consulting in Paris and editor of Security Defense newsletter, said airlines and airports must also know who their employees are. "It's more dangerous to not know the identity of one's staff than of one's passengers," he said. "Staff Since staff are so constant and can have regular access to restricted areas, Establier said they are a greater threat. Iain Jack, who was head of security for British Airways for nearly a decade and now heads his own consulting firm, Carlingwark Consultants, agreed. "The staff searching regime should be as rigorous as that applied to passengers," he said.

But employees' threats to security aren't always intentional, according to Hughes. He pointed out that a large part of hacking is social engineering. Staff can accidentally give out pertinent information that can allow hackers access to airport and airline systems. Hughes said successful hackers have been able to garner passwords and other vital information from employees. As such, employees at all levels need to be aware of the risk of giving out too much information. "It's a combination of best practices and good employee training but also hiring good people that won't be tripped up when circumstances like that present themselves," Hughes said.

Ragnarsson concurred: "The employees need to know what the dangers are so that they become a part of the defence."

Geoffrey Askew, retired head of security and emergency management for the Qantas Group in Australia who now heads security consulting firm, Askew and Associates, said training all employees in some level of behavioural analysis isn't a bad idea. "Technology won't work by itself; it's going to be associated with people," Askew said. "Good housekeeping, staff awareness programmes, training of frontline staff in behaviour analysis to be able to recognise abnormal behaviour and report it is important."

The second part of the human component is the hacker. Understanding who hackers are helps make the threats clearer; however, that's not as easy as it sounds. "One of the most dangerous aspects of cyber threats seems to be that the culprits do not fall into any one category," Ragnarsson said. "Although the ideal hacker is a lonely teenage boy, the evidence seems to indicate that hackers are well-educated, 'respectable' men – although there must also be some women in this group as well." Golubev said many hackers are out only to prove that they can break into a system. Others are out to utilise that access for selfish means. "It is an endless process of struggle between hacker and professional security intelligence," he said. Askew added that hackers are not stereotypical street criminals. Instead hackers are intelligently looking for a way to defeat systems in place. "It would be very naïve to say we have totally secured our IT infrastructures," he said.

"...one of the most dangerous aspects of cyber threats seems to be that the culprits do not fall into any one category..."

Looking Forward

As a relatively new front in aviation security, cyber security is ever-changing. Those involved in the field see a need for other changes to take place. Above all, becoming proactive rather than reactive seems to be the key to combating hackers. "It is getting to a stage where it is intellectual terrorism," said Askew. "We underestimate sometimes the commitment of those out there who have intent to do harm. Hopefully it won't take an incident before we wake up and start to address it as a global industry. We've got a history now of waiting for instances to happen before we respond." Along with that, IT managers need to be properly trained. Many come from military, law enforcement or aviation backgrounds rather than IT backgrounds, according to Askew. "I think to combat that we need to employ IT security experts who are purely focused on the risks and threats associated with cyber crime," he said. That can include reformed hackers or ethical hackers who are going to work for many companies and help them secure vulnerabilities.

Product screens from AirTight Networks

Identifying risks is important, because, as Rauscher pointed out, cyber terrorists are constantly looking for ways to attack that haven't been seen before to catch the industry by surprise. King said one such attack that is growing in popularity but has yet to be seen in airports is a Denial of Service (DoS) attack. Hackers bombard a Web site or server and crash it, which is especially easy to do with a wireless system. A system rendered useless in an airport could have catastrophic consequences. "That's a threat to watch for the future where somebody will disrupt the usage of the network and attack, essentially, the airport's operations that way," King said. "We haven't seen a lot of it yet, but thinking ahead, we've already evolved technology…to block the DoS attacker from utilising air space to attack a network."

And, along with hiring the best staff and understanding the forthcoming risks to computer systems, Hughes said communication about cyber security will be the best tool to prevent cyber terrorism. Unfortunately, that tool is far from being utilised. "There are just a lot of unknowns," he said. "Information sharing overall is pretty poor among both industry players and the government which makes developing solutions very difficult because so many are not publicised or are classified. And there's good reason for that, but it's a careful balance that has to be followed. Getting access to good data is sometimes very, very difficult." Hughes said although sharing information can be tricky, it is important for effective cyber security to progress. "Just very generally, people in the security community are taught not to share information," he said. "That was OK in the Cold War era, but it's not OK in the global internet age…You can't go too far since you don't want to give all your secrets and tactics to your competitors or enemies. But at the same time, the cost of retaining information oftentimes outweighs the benefits." Rauscher agreed. He said some proposals have been made and a movement is beginning to allow companies and industries to share information about how they were compromised in a private arena so others can learn from their experiences. This would avoid damaging the hacked company's reputation or hurting its bottom line. "There's definitely a need for continued cooperation at an international level between the private sector, researchers and also government entities," Rauscher said. "We all are in cyberspace. We're all in this together. Basically, we need to work on these problems and issues together throughout the world." ■

The author is a freelance journalist and copywriter based in Indiana in the United States. She has been the owner of Written Creations, LLC, since founding it in 2004. Along with having more than 500 articles in various local, regional, national and international publications, she also works with clients on marketing and business material. For more information, visit www.writtencreations.com.