RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg No. 187 – 1 September 2015

Cybersecurity in Civil Aviation: Need for Industry-wide Approach

By Eugene EG Tan

Synopsis

Civil aviation is rapidly embracing newer technologies to enable operations to be more efficient. However, ease of use and data availability in civil aviation may pose potential cybersecurity risks to the industry with international implications.

Commentary

ON 7 AUGUST 2015, it was disclosed that the databases of American Airlines (AA) and Sabre Corp., one of the largest clearing houses for travel reservations, were hacked. Taken together with the hacking of United Airlines in July 2015, this revelation shows that the civil aviation industry is increasingly prone to cyberattacks, and contains cybersecurity lapses that need to be addressed.

However, passenger data theft may just be the tip of the iceberg when it comes to cybersecurity in the civil aviation sector. Revenues in the industry top US$388 billion, presenting a tempting target for potential cyber criminals. Revenue streams are not the only target for hackers. The civil aviation industry is also a treasure trove of data, with flight data and personal data being collected by both the airlines and regulators' servers.

Next generation air transportation system

While this data is collected to ensure the physical safety of passengers by securing and verifying the identity of the passenger, the concern is that data collected by hackers could be misused in many ways, including espionage, identity theft and credit card fraud.

In April 2015, the General Accountability Office (GAO) released a study advising the Federal Aviation Administration (FAA) to take a more comprehensive approach towards cybersecurity as it moves toward a NextGen Air Transportation System. The report singled out three main areas for improvement: air traffic control (ATC), avionics, and the roles and responsibilities among FAA offices. These are long term issues that need to be addressed going forward, but with the advance in and the changing nature of information and communications technology (ICT), these are also urgent issues that need robust and present solutions.

Integrated nature of civil aviation

The civil aviation industry is a large and international industry that encompasses many stakeholders, including regulators, airport operators, aircraft and engine manufacturers, and airlines. The industry employs up to 58 million people worldwide in associated jobs, and generates about US$2.2 trillion in GDP yearly. The different sectors in the civil aviation industry are also closely knit, relying on each stakeholder to accurately provide information and services for efficient air operations.

However, as seen in the AA and Sabre cyberattacks, hackers can strike at different stakeholders in the industry. Therefore, the civil aviation industry in Singapore needs to recognise the industry-wide nature of the challenge cybersecurity poses. Parallels to the civil aviation industry can be drawn from the cyberattack on Target in November 2013 where credentials from an air-conditioning vendor were used by hackers to access the Target network, enabling hackers to install undetected malware, and collect credit card details from cashier terminals.

As a large department store, Target handles many transactions daily from both customers and vendors, much like the civil aviation industry with its multiple stakeholders and customers, who may not understand cybersecurity risks. Similarly, with multiple payment and vendor systems in the civil aviation industry, the industry is only as resilient to cyberattacks as its weakest link.

Increasing sophistication of civil aviation technology

The increasing sophistication of ATC systems and aircraft has benefited the civil aviation industry, but has also raised potential threats to the civil aviation industry. Technological advances have made planes much easier to fly, with improved avionics on-board to help with landings and take-offs. Conversely, overreliance on on-board avionics can also cause tragedy in civil aviation.

Newer aircraft are also equipped to provide Internet connection to passengers. While having Internet on-board is a boon for passengers living in the digital age, it is a possible security situation for airlines and regulators. The possibility of unauthorised personnel connecting to an aircraft avionics system through Wi-Fi in the plane was flagged as a potential blind spot in a GAO report published in April 2015 on the FAA's approach toward NextGen cybersecurity.

Increasingly, air traffic control systems are also modernising to complement and communicate better with aircraft. Improved NextGen systems allow more data to be collected; enable data sharing between air traffic control and aircraft; allow flights to be better routed; and provide more efficient airport management.

The downside of NextGen technology is the magnitude of air service disruption should the system fail. For example, a computer glitch at an air traffic centre in Virginia caused more than 440 flights to be cancelled along the East Coast of the United States in August 2015. While not a cyberattack, this incident showed the vulnerability of NextGen technology in civil aviation.

Implications for regional civil aviation industry

As an international aviation hub, Singapore has kept these cybersecurity threats and blind-spots in view, but challenges remain. Although a small state, Singapore's flight information reporting zone extends well into the South China Sea, making technology vital to Singapore's ATC systems.

NextGen technology – LORADS III – is helping Singapore create a more efficient air traffic management system, especially with planned increases in capacity in the near future. However, ATC systems need to be resilient against cybersecurity threats to ensure the verity of the data produced and provided is not compromised.

While Singapore can afford these advanced systems, other states in the region may not have such capabilities in aircraft monitoring. This asymmetry in capabilities may pose difficulties toward air traffic growth in the wider region and raises questions on the ability to process and provide data to aircraft passing through the region. These are security questions that need to be addressed as a region, and with the ASEAN Single Aviation Market (ASAM) scheduled to be rolled out by the end of 2015, ASEAN needs to ensure that these air traffic monitoring systems are also adequately protected against cyber mischief.

In conclusion, the challenge posed by cybersecurity to the civil aviation industry is massive, and with ASAM becoming a reality by the end of 2015, the civil aviation industry must recognise that the responsibility of cybersecurity is indivisible and becoming more international in nature.

Eugene EG Tan is an Associate Research Fellow at the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University in Singapore.