Air Safety Cyber Security: Why Cyber Security is a Threat for Air Safety

submitted for the ISASI Rudolf Kasputin Memorial Scholarship 2019

Nur Amalina Jumary

University of New South Wales

1613 words

Aviation a ‘System-of-Systems’

Aviation today uses complex, integrated systems of information and communication technology to facilitate its daily global operations. At the Thirteenth Air Navigation Conference by the International Civil Aviation Organization (ICAO) in 2018, aviation was conceptualised as a ‘system-of systems’. This concept is defined as a collection of different sets of systems consisting of people, products and processes required for the completion of tasks, none of which are dispensible. Such a system has been enabled by digital technology. Digitalisation automates processes by connecting digital technology, information, and people. The digitalisation of aviation has allowed for an increased level of operational efficiency and the means to keep up with increasing commercial demands of international air travel. Despite optimising operations, digitalisation has introduced new vulnerabilities to the industry, namely in the domain of information security or cyber security. The interconnectedness of the systems means an increased level of interaction with different information systems, beyond what the industry has traditionally defined as its security parameter (Boeing, 2012), which leaves it at risk of new security threats that may potentially become a concern for air safety.

Information Security in Aviation

Innovations in the design and manufacturing process have brought about ‘E-enabled’ aircraft that are built with onboard information and communications technology that communicate with external networks to exchange data during flight, while on the ground or anywhere in the world (ALPA, 2017). E-enabled systems present on widely-used commercial aircraft like the Airbus 380 and the Boeing 787 Dreamliner communicate with numerous networks around the globe, all with varying degrees of security. At present, there are no common cyber standards for aviation systems (AIAA, 2013) which means the risks present in data communication, such as the transfer of flight and system data using wireless technology, or maintenance and diagnostic functions that are performed remotely, are yet to be effectively managed.

The threat to air safety as a result of vulnerable information security is far from novel. In 2006, the Federal Aviation Administration (FAA) was forced to shut down a portion of its Air Traffic Control (ATC) systems after a cyber-attack caused disruption in its mission support functions. An audit of the FAA's air traffic control cyber security protection measures found that the use of commercial software and Internet Protocol-technologies in a bid to modernise operations, put the system at a high security risk as operations were not properly secured to prevent unauthorised access. An Inspector General report presented to the FAA by the U.S Department of Transportation warned that it is a matter of time before attacks to ATC systems would do serious harm to ATC operations (Baldor, 2009). The reliance of aircraft in communicating with ATC is a vital aspect of air safety, thus any threats that could potentially compromise the system's integrity should be properly identified and managed.

Although there is yet to be a serious cyber security incident or accident relating to ATC more than a decade since the incident discussed earlier, in 2015, a security expert in United States of America was detained after allegedly hacking into the in-flight entertainment (IFE) system on United Airline's Boeing 737-800 and on one occasion, had successfully overwritten a code to issue a "climb" command. In 2017, another cyber security expert working with Homeland Security successfully hacked into a parked Boeing 757 through radio frequency communications (Flight Safety Australia, 2017). The recurrence of a cyber-attack indicates that there has not been enough progress made by the aviation community or support from governments to expand the notion of safety as the industry has known it to encompass systems onboard and on the ground with strong information security. The FAA has taken initiatives to improve information security by tasking its Aviation Rulemaking Advisory Committee to provide cyber security recommendations which included testing and updating of cyber security protections (FAA, 2016). On the legislative level, the Cyber AIR Act was reintroduced in Congress in 2017 but has yet to be enacted (Govtrack, 2017). The aviation industry is cognizant of the threats and the consequences of a lax information security system, but reforms and changes are made at a rate much too slow for the industry to have any regulatory or legislative framework to effectively manage the safety risks that have been identified.

Challenges for Investigators

Adopting a generative attitude to air investigation

Air safety investigators are responsible for providing recommendations to improve air safety after ascertaining causes of aviation accidents or incidents with the aim to prevent similar occurrences in the future. Inherent to this investigation philosophy is the use of a proactive systems safety approach to air safety (Dempsey, 1999), even though practically investigators are carrying out investigations post-event. With the security threats and hazards that surround cyber security and safe air transport, this approach is not enough, as investigators have to launch into a retrospective investigation driven by data collected through research. To date, there has not been a major occurrence that has significantly compromised air safety as a result of a cyber security attack. However, this lack of precedence is compensated by a vast collection of occurrences captured through the Mandatory Occurrence (Incidence) Reporting systems established by ICAO Annex 13. The challenge for investigators is to adopt a generative attitude (Hudson, 2001) where they would access and review large volumes of data and proactively review occurrence data to identify and quantify the threats due to lapse in information security. This allows investigators to put forth recommendations to improve air safety cyber security.

Training challenges due to the need for an enhanced skill set

Another challenge that air safety investigators face is the need to undergo further training in order to acquire the relevant skills to identify cyber security breaches. Air safety investigators have a high level of technical skill and knowledge in the aviation domain (Braithwaite & Nixon, 2018), but an investigation is a complex task that draws upon a broad range of skills. The Product Security Director of Airbus Americas revealed that Airbus had not equipped their aircraft with any cyber security information as pilots surveyed by the manufacturer preferred not to be informed of such threats during flight (ALPA, 2017), possibly due to the perceived increase in workload. In the event of a total hull loss the flight data recordings may not reveal accurately the state of events that led to the accident if there was an external presence that was able to overwrite the pilots' inputs. While there is value in having investigators know what they are looking for in regards to causes of incidents or accidents, there is equal value in having investigators be aware of what they do *not* know given a novel situation.

An important facet of training that has to be acknowledged is the limitation of training itself. It is highly misleading to expect investigators to have expertise in all aspects of aviation ranging from human factors to aircraft systems and cyber security. The use of Subject Matter Experts (SME) is used in the industry exactly because it is unreasonable to expect investigators to have both depth and breadth of knowledge in all areas of aviation especially in its fast-changing nature. Airbus also faces a challenge of finding talent that have dual-expertise in aircraft design and cyber security (ALPA, 2017), and investigation bureaus face a similar challenge with their investigators. In the area of cyber security, the call to equip investigators with an enhanced skill set is part of a 'total-system' approach. This will ensure that aviation evolves in tandem with the systems that comprise it in order to establish a cyber security culture where cyber threats are recognised and communicated, and importantly where the risks are managed effectively.

Integrating Information/Cyber Security Management and Safety Management Systems

A strategic way in moving forward is to adopt a proven methodology; one the aviation industry has used in the past. Aviation has benefited from implementing a robust, systematic approach to managing safety. The way the industry involves organisational structures, policies and procedures, and accountabilities to control safety risks in operations has been studied and replicated in other industries like healthcare (Kapur, Parand, Soukup, Reader, & Sevdalis, 2016), and even cyber security at its nascent stage (Seawright, 2018). Having an "Information/Cyber Security Management System" integrated to the current Safety Management System (SMS) would allow the industry to continue managing threats that have been previously identified as well as new ones that arise through innovation in aviation. The advent of this digital-era of aviation brings with it new hazards and threats, all of which do not appear to be fully realised. Thus, having an Information/Cyber Security Management System which responds to the new vulnerabilities the industry faces integrated with the existing SMS would be an effective approach in managing safety risks.

In summary, there is a general consensus in the industry that a harmonised approach is the most effective way to manage the threats relating to information security in aviation (Boeing, 2012). Individual organisations like the European Aviation Safety Agency (EASA) have made amendments to make it mandatory for manufacturers that are seeking certifications to provide evidence that threats leading to unauthorised access of electronic information or systems are addressed (2019). Similarly, Boeing is establishing a Cyber Technical Centre to support the cyber security needs of its customers (2012). Efforts made by individual agencies are important, but synchronising these individual efforts to establish a strong cyber security culture would effectively manage information security concerns, thereby maintaining air safety. Central to this system safety approach is providing the necessary education for investigators to gain the knowledge to identify and recognise threats that are contemporary to the industry, and subsequently the proper trainings for them to acquire skills to provide recommendations to improve air safety.

References

Air Line Pilots Association. (2017). Cybersecurity Concerns in Today's Aviation Environment. Retrieved on 21 March 2019 from https://www.youtube.com/watch?v=V7SDoHW4vCI&t=3866s

American Institute of Aeronautics and Astronautics. (2013, August). *A Framework for Aviation Cybersecurity*. Paper presented at the AIAA Aviation Technology, Integration, and Operations (ATIO) Conference, Los Angeles, CA: American Institute of Aeronautics and Astronautics.

Baldor, L. (2009, May 6). Audit: Air traffic systems vulnerable to attack. The Associated Press.

Boeing. (2012). *Aero QTR_03.12. Securing Airline Information on the Ground and in the Air*. Retrieved on 21 March 2019 from https://www.boeing.com/commercial/aeromagazine/articles/2012_q3/5/

Dempsey, P. (2010). Independence of Aviation Safety Investigation Authorities: Keeping the Foxes from the Henhouse. *Journal of Air Law and Commerce. 75*(1), 2223-2282. European Union Aviation Safety Agency. (2019). Aircraft Cybersecurity. Retrieved on 21 March 2019 from https://www.easa.europa.eu/sites/default/files/dfu/NPA%202019-01.pdf

Federal Aviation Administration. (2016). A Report from the Aviation Rulemaking Advisory Committee (ARAC) Aircraft System Information Security / Protection (ASISP) working group to the Washington, DC: Author.

Flight Safety Australia. (2017, November 14). Government officials hack airliner. Retrieved on 22 March 2019 from https://www.flightsafetyaustralia.com/2017/11/government-officials-hack-airliner/

GovTrack. (2017). *S. 679 (115th): Cyber AIR Act.* Retrieved on 24 March 2019 from https://www.govtrack.us/congress/bills/115/s679

Hudson, P. (2001). Safety management and safety culture the long, hard and winding road. *Occupational Health and Safety Management Systems: Proceedings from the First National Conference (pp.3 – 22)*, Sydney, AUS: University of Western Sydney.

International Civil Aviation Organisation. (2018). Considerations About Cybersecurity in Aviation. Retrieved on 21 March 2019 from https://www.icao.int/Meetings/anconf13/Documents/WP/wp_160_en.pdf

Kapur, N., Parand, A., Soukup, T., Reader, T., & Sevdalis, N. (2016). Aviation and healthcare: a comparative review with implications for patient safety. *Journal of The Royal Society of Medicine Open, 7(1),* 1-10.

Nixon, J., & Braithwaite, G. (2018). What do aircraft accident investigators do and what makes them good at it? Developing a competency framework for investigators using grounded theory. *Safety Science, 103,* 153-161.

Seawright, S. (2018, Aug 14). Applying Aviation Safety Practices to Cybersecurity. Retrieved on 21 March 2019 from https://connectedaviationtoday.com/applying-aviation-safety-practices-cybersecurity/