NOT YOUR GRANDDADDY'S AVIATION INDUSTRY: THE NEED TO IMPLEMENT CYBERSECURITY STANDARDS AND BEST PRACTICES WITHIN THE INTERNATIONAL AVIATION INDUSTRY

Jennifer Ann Urban[1]

"People ask me all the time, 'What keeps you up at night?' And I say, 'Spicy Mexican food, weapons of mass destruction and cyber attacks [sic]. . . .'"[2]
– Dutch Ruppersberger, United States Congressman

ABSTRACT

The international aviation industry's increased usage of technology has generated new cybersecurity concerns that cannot be ignored. The lack of a global cyber governance makes it difficult to enforce cybersecurity policies. An industry-wide, multi-stakeholder approach must be taken to develop international standards and best practices for assessing and managing cybersecurity risks.

This paper will first address the impact cyber threats and attacks have had on the aviation industry. Next, it will explain how technologies like the Next Generation Air Transportation System (NextGen) and aircraft wireless internet have made cybersecurity more vulnerable. Third, it will present the basic cybersecurity framework and analyze past attempts by international aviation organizations to execute cybersecurity risk management programs. Finally, it will offer better solutions to evaluate and handle cybersecurity risks in the international

[1] Jennifer Urban is an associate in the Transportation and Trade Group of Cozen O'Connor. She earned her LL.M. in Air and Space Law, J.D., M.B.A., and B.A. at the University of Mississippi. Ms. Urban would like to thank Professor P.J. Blount for his helpful insights and support.

[2] Steven Hsieh, *Congress Is Trying to Kill Internet Privacy Again*, ROLLING STONE (Feb. 13, 2013), http://www.rollingstone.com/politics/news/congress-is-trying-to-kill-internet-privacy-again-20130213.

aviation industry and suggest that these solutions be combined. Both public sector and private sector support for international standards and best practices is required to significantly strengthen cybersecurity for the entire global aviation industry.

INTRODUCTION 63
BACKGROUND 65
NEW TECHNOLOGIES BRING NEW VULNERABILITIES 70
NextGen 71
Aircraft Wi-Fi 76
BASIC CYBERSECURITY FRAMEWORK AND PAST ATTEMPTS AT IMPLEMENTATION OF PLANS 79
Executive Order 13636: Improving Critical Infrastructure Cybersecurity 79
Basic Cybersecurity Framework 81
Past Attempts by International Organizations to Address Aviation Cybersecurity Threats 83
SOLUTIONS TO CYBERSECURITY THREATS 85
International Standards 86
Information Sharing 88
Training Programs 91
CONCLUSION 93

INTRODUCTION

Today, most people will do whatever they can to get out of having to call an airline, because they know that no matter what issue they need assistance with, they will likely have to go through multiple lists and suffer through long wait times. It is hard, if not impossible, for many people to remember the pre-digital age where calling the airline was pretty much the only way for a customer to interact with an airline, besides being at the airport.[3] When the telephone was the main mechanism used to contact an airline, no one was really worried about cyber threats occurring due to the use of this pre-digital technology.[4] Instead, the main threats to the

[3] *The Way We Used to Travel: 12 Ways Travel Has Changed in the Digital Age*, THE HUFFINGTON POST (Feb. 22, 2014), http://www.huffingtonpost.com/2014/02/22/the-way-we-used-to-travel_n_4818247.html.

[4] *See* Heather E. Reser, *Airline Terrorism: The Effect of Tightened Security on the Right to Travel*, 63 J. AIR L. & COM. 819, 823–28 (1998) (using history of airline terrorism to demonstrate that security threats have largely been comprised of terrorist hijackings and bombings); *See also* Bernard Lim, *Aviation*

aviation industry were the traditional terrorist hijackings and bombings of airports and aircrafts.[5] No one likely wants to go back to the day of having to call the airline, because the Internet is a much simpler and efficient mechanism. However, people must accept that the use of this post-digital technology brings both perks and potential threats to the aviation industry.

Although technology usually improves efficiency and safety mechanisms in everyday processes, the increase in its use also creates new security vulnerabilities.[6] One may think the potential for terrorist attacks where planes are physically crashed is the main threat that industry professionals face, but cyber-attacks can be just as deadly and harmful, if not more so. According to a survey conducted by PricewaterhouseCoopers, "85 percent of airline CEOs expressed concern about [cybersecurity] risk versus 61 percent of CEOs in other industries. . . ."[7] Even though cyber-attacks have not been as publicized as physical attacks, many have occurred in recent years. From the 2008 Spanair accident, where malware infected the central computer system of the Spanish government's Civil Aviation Accident and Incident Investigation Commission, to the 2015 hacking of the Malaysian Civil Aviation Department's website, cyber-attacks on aviation are taking place around the world.[8] This paper will argue that the international aviation industry needs to adopt recommendations for general standards on how to assess and manage cybersecurity risks, while also developing best practices to make the aviation community

Security – Emerging Threats from Cyber Security [sic] *in Aviation – Challenges and Mitigations*, J. OF AVIATION MGMT. 83, 83 (2014), http://www.saa.com.sg/saaWeb2011/export/sites/saa/en/Publication/downloads/EmergingThreats_CyberSecurityinAviation_ChallengesandMitigations.pdf (discussing how security threats have become more difficult to handle due to the increased use of and dependence on computer-based and information technology systems, which demonstrates that when these systems were not in use, in the pre-digital age, the security threats were different).

[5] Reser, *supra* note 4.

[6] 4.2 PRICEWATERHOUSECOOPERS, AVIATION PERSPECTIVES 2016 SPECIAL REPORT SERIES: CYBERSECURITY AND THE AIRLINE INDUSTRY 2 (2016 ed. 2016), https://www.pwc.com/ (copy the title as seen in this footnote or manually type "Aviation Perspectives 2016 Special Report Series: Cybersecurity and the Airline Industry" into the search bar at the top right corner of the website, then click on the first link, titled "Cybersecurity risk prevention within the airline industry: PwC," and then proceed to download "Aviation Perspectives: Volume 4.2").

[7] *Id.* at 3.

[8] SENSECY, CYBER THREATS TO THE AVIATION INDUSTRY – 2014 8–9, http://www.export.gov.il/files/hls/CyberThreatstotheAviationIndustry.pdf?redirect=no&utm_source=InforuMail&utm_medium=email&utm_campaign=HLS+%26+CYBER+2016 (last updated May 5, 2015).

more secure. By engaging as an entire industry to confront this cybersecurity risk, aviation as a whole will become much safer.

This paper will begin with background information on how the aviation industry has been impacted by cyber threats. In order to fully understand the many ways technology can affect the aviation industry, and open it up to potential new threats, the second section explains two key aviation technologies: NextGen and aircraft wireless Internet (Wi-Fi). These two technologies exemplify different parts of the aviation industry from the general navigation systems to customer interaction with the aircraft itself.[9] The third section discusses the basic cybersecurity framework and past attempts to implement cybersecurity risk management plans. International institutions, such as the International Civil Aviation Organization (ICAO) and the International Air Transport Association (IATA), have made efforts in the past to address cybersecurity issues.[10] These programs will be analyzed to determine better-recommended solutions to cybersecurity problems. The fourth section proposes solutions on how to assess and manage cybersecurity risks for the international aviation industry. These solutions include international standards, information sharing, and training programs. The paper concludes with a recommendation to combine the methods suggested to minimize cybersecurity risks in aviation.

BACKGROUND

Cybersecurity is defined by the International Telecommunication Union as the

> collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. . . . Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.[11]

The U.S. National Academy of Sciences defines cyber-attacks as

---

[9] *See* Adam Clark Estes, *Every Major Airline's Wifi Service, Explained and Ranked*, GIZMODO (May 4, 2015), http://gizmodo.com/every-major-airlines-wifi-service-explained-and-ranked-1701017977 (discussing how airplanes use both towers and satellites in order to deliver data to smartphones).

[10] Lim, *supra* note 4, at 85–86.

[11] *Overview of Cybersecurity*, INT'L TELECOMM. UNION 2 (April 18, 2008), https://www.itu.int/rec/T-REC-X.1205-200804-I (click on the PDF link for the desired language).

"deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[12] Cyber-attacks can reach a much broader target because they are not restrained by traditional physical boundaries.[13] Past cyber-attacks have not been limited to one specific region, but instead have taken place around the world.[14] The aviation industry's increasing dependence on telecommunication networks and technological programs makes it a large target for cyber-attacks.[15]

On August 20, 2008, Spanair flight 5022 crashed right after taking off from Madrid-Barajas International Airport.[16] The crash killed 154 people and left 18 survivors.[17] The cause of the crash was due to a malware infection in the aircraft's central computer system that was in charge of monitoring any technical problems on board.[18] Because of the malware, the computer system was not able to warn of three defects within the aircraft.[19] If the computer system had been functioning properly, it would have been able to warn the pilots about the defects, which would have likely stopped the aircraft from taking off.[20] The malware was determined to be a Trojan horse that could have gotten onto the system multiple ways, even simply by accidentally opening one infected file.[21] Cyber Defense Agency President, O. Sami Saydjari, claimed, "[a]ny computer that is connected to a network is vulnerable to a malware infection. Standards have not been set to protect critical infrastructure."[22]

---

[12] NATIONAL RESEARCH COUNCIL OF THE NATIONAL ACADEMIES, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 1 (William A. Owens et al. eds., 2009).

[13] MARIE-HELEN MARAS, TRANSNATIONAL SECURITY 135 (2015).

[14] *Cybersecurity: A Global Issue Demanding a Global Approach*, UNITED NATIONS DEP'T OF ECONOMIC AND SOCIAL AFFAIRS (Dec. 12, 2011), http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html.

[15] Bob Cheong, *Cyber Security* [sic] *at Airports*, LOS ANGELES WORLD AIRPORTS 4, http://www.aci-na.org/sites/default/files/ncheong-cybersecurity-bit.pdf (last visited Sept. 26, 2016).

[16] Leslie Meredith, *Malware Implicated in Fatal Spanair Plane Crash*, NBC NEWS, http://www.nbcnews.com/id/38790670/ns/technology_and_science-security/t/malware-implicated-fatal-spanair-plane-crash/#.VyeAs2Z1Zms (last updated Aug. 20, 2010).

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] Meredith, *supra* note 16.

According to Los Angeles World Airports' former Chief Information Security Officer, Bob Cheong, "[i]ncreasing numbers of critical business systems are interconnected with partners and customers on the [I]nternet which present[s] a danger of cyber attacks [sic] on these systems."[23] For example, from July 2010-July 2011, the Los Angeles World Airports blocked approximately 2.9 million cyber-hacking attempts.[24] The more interconnected any of the technological systems used in aviation are, the bigger potential there is for a cybersecurity breach.[25] One way to combat the interconnectedness vulnerability is to compartmentalize the different systems and networks.[26] By compartmentalizing the systems, it prevents a cybersecurity breach in one system from affecting any other systems or even the entire company's main network.[27]

On July 26, 2013, both of Istanbul's main airports, Istanbul Atatürk and Sabiha Gökçen, were attacked by malware.[28] The malware affected the airports' passport control systems and attempted to steal information from those systems.[29] Luckily, in this incident, no deaths occurred from the effects of the malware, although passengers were forced to stay in line for hours and many

---

[23] Cheong, *supra* note 15; Bob Cheong, LINKEDIN, https://www.linkedin.com/in/bobcheong (last visited Sept. 27 2016) (showing that Mr. Cheong is now the Chief Information Security Officer for Riverside County).

[24] *Cybersecurity for Airport Systems*, INTELLIGENT TRANSPORTATION SOCIETY OF CALIFORNIA (September 22, 2015), http://www.itscalifornia.org/15techsessions (follow link provided in this footnote, scroll down until "Technical Session 7: White Hats and Black Cats: Staying Lucky in the Changing World of its Cybersecurity," and then click on the link designated as "Airport Security Technology").

[25] Dr. Detlev Gabel et al., *Cyber Risk: Why Cyber Security* [sic] *is Important*, WHITE & CASE LLP (July 1, 2015), http://www.whitecase.com/publications/insight/cyber-risk-why-cyber-security-important?s=Cyber%20Risk:%20Why%20Cyber%20Security%20is%20Important.

[26] Dominic Wai & Aaron Bleasdale, *Hong Kong: How to Respond to Cybersecurity Threats*, GLOBAL COMPLIANCE NEWS (Dec. 8, 2014), http://globalcompliancenews.com/hong-kong-how-to-respond-to-cybersecurity-threats/.

[27] *Id.*

[28] John Leyden, *Airports' Passport Controls Shut Down by "Malware" - Report*, THE REG. (July 31, 2013), http://www.theregister.co.uk/2013/07/31/istanbul_airport_chaos_malware_blamed/; *see also* Pierluigi Paganini, *Istanbul Ataturk International Airport Targeted by a Cyber Attack* [sic], SECURITY AFF. (July 28, 2013), http://securityaffairs.co/wordpress/16721/hacking/istanbul-ataturk-international-airport-targeted-by-cyber-attack.html (discussing how the cyperattack specifically targeted the passport control system at Istanbul Ataturk International Airport).

[29] Paganini, *supra* note 28.

flights were delayed.[30]

In September 2013, Japan Airlines suffered a cyber-attack on its Customer Information Management System.[31] The virus attacked computer terminals in the airline's network.[32] After gaining access to the system, the hackers were able to steal up to 750,000 frequent-flier program members' personal information.[33] During the cyber-attack investigation, Japan Airlines was unable to determine the exact external server where the stolen data was sent, but it did figure out that the server was located in Hong Kong.[34] While a cyber-attack on one airline is horrible, due to the interconnectedness and alliances between airlines, a single attack can affect multiple airlines.[35] Japan Airlines is one of fifteen member airlines of the Oneworld Alliance, LLC.[36] Although, in this case, there did not seem to be any effects on other airlines within the alliance, it brought to light the possibility of this type of problem occurring in the future.[37]

On March 8, 2014, the disappearance of Malaysia Airlines flight MH370 occurred with 239 people on board.[38] The next day, there was a cyber hack on Malaysia's Civil Aviation Department, the National Security Council, and Malaysia Airlines.[39] Government officials received an e-mail, containing what looked like a news article, stating that the missing flight had been found, with the e-mail attachment disguised as a PDF, and when clicked, released

---

[30] *See* Leyden, *supra* note 28 (noting that the security problems only caused long lines and delayed flights, thus not causing any deaths).

[31] Althea C. Bartley, *Cybersecurity: Regional Challenges*, MANAGER AVIATION SECURITY & FACILITATION 7 http://www2010.icao.int/SAM/Documents/2015-AVSECFALRG/2.5%20CYBERSECURITY%20Regional%20Challenges%20-%20English.pdf (last visited May 2, 2013); Megumi Fujikawa, *Japan Airlines Reports Hacker Attack*, THE WALL ST. J. (Sept. 30, 2014), http://www.wsj.com/articles/japan-airlines-reports-hacker-attack-1412053828#:jmSkNkySbQp2JA.

[32] Fujikawa, *supra* note 31.

[33] *Id.*

[34] *Id.*

[35] THE INT'L COORDINATING COUNCIL OF AEROSPACE INDUSTRIES ASSOCIATIONS, *Cyber Security* [sic] *for Civil Aviation* 3 (Int'l Civ. Aviation Org., Working Paper No. 122, 2012), http://www.icao.int/Meetings/anconf12/WorkingPapers/ANConfWP122.1.1.ENonly.pdf.

[36] *Member Airlines – Overview*, ONEWORLD ALLIANCE, LLC, https://www.oneworld.com/member-airlines/overview (last visited May 3, 2016).

[37] Fujikawa, *supra* note 31.

[38] Jiaxi Lu, *Chinese Hackers Reportedly Took Classified Data on MH370 a Day After it Went Missing*, THE WASH. POST (Aug. 20, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/08/20/chinese-hackers-reportedly-took-classified-data-about-mh370-a-day-after-it-went-missing/.

[39] Bartley, *supra* note 31, at 8; Lu, *supra* note 38.

malware onto the computer system.[40] The information stolen from Malaysia's Civil Aviation Department by the malware was supposedly sent to a computer in China.[41]

Malaysia Airlines was again targeted by a cyber-attack in January 2015.[42] When the airline's website URL address was imputed, the user would be re-directed to a website belonging to the hacker.[43] Originally, when users attempted to visit the airline's website, they were re-directed to a page that stated "404 – Plane Not Found," and the website tab stated "ISIS will prevail."[44] Later, when users imputed the airline's URL address, it re-directed them to a website that stated "Hacked by Lizard Squad – Official Cyber Caliphate."[45]

These past incidents exemplify how a country's critical infrastructure can be harmed through a cyber-attack. According to award-winning cybersecurity author, Kim Zetter, "[i]n broad terms, critical infrastructure refers to any system of high importance to the safety and operation of the country. . . . The U.S. government has actually defined sixteen sectors of critical infrastructure. . . ."[46] Most countries have their own definitions of critical infrastructure, but overall these definitions are similar enough to understand that society as a whole must be protected.[47]

---

[40] Nicholas Cheng, *Hacker Targets Info on MH370 Probe*, THE STAR ONLINE (Aug. 20, 2014), http://www.thestar.com.my/news/nation/2014/08/20/hacker-targets-info-on-mh370-probe-computers-of-officials-infected-with-malware/.

[41] *Id.*

[42] Yvonne Lim, *Hacker Group "Cyber Caliphate" Targets Malaysia Airlines*, TODAY (Jan. 26, 2015), http://www.todayonline.com/world/asia/hacker-group-cyber-caliphate-targets-malaysia-airlines.

[43] *Id.*

[44] *Id.*

[45] *Id.*

[46] Kim Zetter, *Hacker Lexicon: What Counts as a Nation's Critical Infrastructure?*, WIRED ENT. (Feb. 16, 2016, 7:00 AM), https://www.wired.com/2016/02/hacker-lexicon-what-counts-as-a-nations-critical-infrastructure/; *see also Kim Zetter*, WIRED ENT., https://www.wired.com/author/kimzetter/ (last visited Sept. 28, 2016) (providing a short biography of Ms. Zetter).

[47] The United Kingdom defines critical infrastructure as "those assets, services and systems that support the economic, political and social life of the UK whose importance is such that loss could: (1) cause large-scale loss of life; (2) have a serious impact on the national economy; (3) have other grave social consequences for the community; or (4) be of immediate concern to the national government." MARAS, *supra* note 13, at 152. In comparison, critical infrastructure in Canada is defined as "physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Canadians of the effective functioning of governments in Canada." *Id.* at 152–3.

The United States has classified transportation systems, which necessarily include aviation systems, as critical infrastructure.[48] One reason it is important to note that aviation is considered part of the critical infrastructure, in the United States, is because the government is committed to protecting all critical infrastructure from harm, even if private actors are involved in that industry.[49] According to President Obama's 2009 Cybersecurity Report, "[t]he common defense of privately-owned critical infrastructures from armed attack or from physical intrusion or sabotage by foreign military forces or international terrorists is a core responsibility of the Federal government."[50] Although the government will defend the critical infrastructure, due to the high level of private sector involvement in aviation, the government cannot require the industry to implement certain security measures.[51] Zetter further explained that the government's role will be to "advise best practices, share threat intelligence with [critical infrastructure], and provide forensic and recovery assistance after an attack."[52] This perfectly portrays the reason to have all members of the aviation industry involved, both the private sector and the public sector, in developing the best ways to combat cyber threats to technologies used within this industry.[53]

NEW TECHNOLOGIES BRING NEW VULNERABILITIES

The aviation industry's use of advancing technologies establishes an interconnected framework. For example, airlines have transitioned from actual airline employees aiding travelers in all steps of the booking and check-in process to an overall online registration system.[54] An airline's online registration system interacts with the airport's Informational Technology (IT)

---

[48] Zetter, *supra* note 46.

[49] *Id.*

[50] *Id.*; *see also Cyberspace Policy Review*, THE WHITE HOUSE 28, https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (last visited Sept. 28, 2016) (reviewing the nation's current cybersecurity and what steps should be taken to ensure the strongest protection against any and all digital threats).

[51] Zetter, *supra* note 46.

[52] *Id.*

[53] *See id.* (concluding that the private and public sectors working together will protect against cyber hacks, and that this should be encouraged).

[54] Admin, *Can Fully Automated Self-Serve Passenger Check-In Systems Make Travel Easier?*, TRAVELERS UNITED (July 28, 2014), https://travelersunited.org/getting-there/can-fully-automated-self-serve-passenger-check-in-systems-make-an-traveler-easier/.

infrastructure when passengers go to check in at the airport.[55] Although most airlines have their own software and computers, their check-in kiosks and facilities will likely use an airport's network and Internet.[56] Due to this interconnectedness through the airport's IT infrastructure, a cyber-attack on one airline's check-in terminal could potentially threaten all other airlines using the same network.[57] It also does not help alleviate cybersecurity problems when each airline can have its own online registration system, because it creates a lack of uniformity, and a multitude of systems.[58] An international standard regarding how airlines should limit their technological interconnectedness to the airport and other airlines would help minimize cyber threats aimed at online registration systems.

Although there have been many technological advancements in the aviation industry, the two key technologies that this paper will discuss are the Next Generation Air Transport System (NextGen) and aircraft Wi-Fi. Reliance on these two new technologies shows how different parts of the air travel process have become susceptible to cybersecurity vulnerabilities.[59]

NextGen

Historically, the Air Traffic Control[60] system (ATC) was the ground-based radar program that managed air traffic.[61] Due to the

---

[55] RANDALL J. MURPHY ET AL., GUIDEBOOK ON BEST PRACTICES FOR AIRPORT CYBERSECURITY 16 (2015).

[56] *See id.* (though not discussing check-in kiosks specifically, it is reasonable to infer that check-in kiosks would also use an airport's network and Internet).

[57] *See id.* at 15–16 (if individual airlines are connected on the same airport network, it's logical to conclude that a cyber-attack specific to one airlines could impact other connected airlines).

[58] 4.2 PRICEWATERHOUSECOOPERS, *supra* note 5, at 4 (suggesting that industry-wide, global, and uniform approaches and standards will be more efficient in protecting against cyber attacks than each airline having its own systems and figuring out how to protect against cyber attacks alone).

[59] MURPHY ET AL., *supra* note 55, 16 ("Furthermore, with the implementation of the Federal Aviation Administration's (FAA's) Next Generation Air Transportation System (NextGen) Program, as well as the ongoing automation of aviation-related systems, the number of systems of concern to airports is growing").

[60] Air Traffic Control is "[a] service operated by appropriate authority to promote the safe, orderly and expeditious flow of air traffic." *Air Traffic Management Glossary of Terms*, FED. AVIATION ADMIN., https://www.fly.faa.gov/FAQ/Acronyms/acronyms.jsp (last visited Sept. 29, 2016).

[61] Dr. William B. Coyne, *NEXTGEN and SESAR (Single European Sky ATM Research) – The Future of Air Traffic Management*, 1.7 INT'L. J. SCI. COM. & HUMAN. 126, 126 (2013) (discussing how NextGen will be converting ground-

continual increase of air traffic, the ATC is no longer adequate, and new systems are being implemented.[62] The Federal Aviation Administration (FAA) developed NextGen, a satellite-based system, as a way to better handle the increase in air traffic.[63] Europe has also implemented a satellite-based air traffic management program called the Single European Sky ATM Research (SESAR).[64]

ATC uses radar technology that sends a signal to an aircraft for operators on the aircraft to respond to and identify the aircraft.[65] The radar is not continuous and instead does a sweep about every five to ten seconds depending on the type of airspace to determine an aircraft's position.[66] Because the radar signal is not continuous, there is a lapse in time every few seconds where an aircraft's exact location is unknown to the ATC.[67] A few seconds may not seem like a long enough amount of time for this to matter, but an aircraft's speed can allow its location to change enough within this time period to cause issues with other aircrafts.[68] Due to the uncertainty surrounding the exact aircraft location, the aviation industry has required that airspaces of about eight to ten nautical miles be left between aircrafts.[69] The need for these large airspaces between planes is inefficient and limits the number of aircrafts that can adequately use that airspace.[70]

According to the National Aeronautics and Space Administration's (NASA) NextGen Project Manager, Leighton Quon, ATC required that

> [an] [a]ircraft generally fly [sic] indirect . . . paths over a series of ground-based radio beacons. Controllers "watch" the progress of the flights on radar and direct the aircraft individually by radio if they need to alter their paths. The efficiency of a flight route is very limited by the old radio, ground based [sic] beacons and radar

---

based technologies, like the ATC system, into satellite-based technologies); Peter S. Green, *America's Air Traffic Control System is Finally Going Digital*, FOX BUS. (Sept. 28, 2015), http://www.foxbusiness.com/features/2015/09/28/america-s-air-traffic-control-system-is-finally-going-digital.html.

[62] Coyne, *supra* note 61.

[63] *Id.*

[64] *Id.*

[65] Megan Coontz McAllister, Note, *Maximizing Safety under NextGen: Apportionment of Duty, the FTCA, and Policy in Aviation*, 13 J. TELECOMM. & HIGH TECH. L. 129, 131 (2015).

[66] *Id.*

[67] *Id.*

[68] *Id.*

[69] *Id.* at 132.

[70] *Id.*

technology.[71]

The efficiency problems under ATC will be fixed by satellite-based systems such as NextGen, which do not require aircrafts to fly over ground stations.[72] The satellite-based system that NextGen employs is the Automatic Dependent Surveillance-Broadcast, which uses GPS to determine the exact accurate location of an aircraft.[73] Both controllers and pilots will be able to access this real-time aircraft positioning information through the NextGen Data Communication System rather than by radio.[74] NextGen will also have computers, rather than people, determining the "most efficient paths to fly while still keeping a safe distance from other aircraft[s]."[75]

The U.S. Government Accountability Office (GAO) was asked by Congress to review the NextGen system, in order to identify potential cybersecurity risks generated by the system and to give recommendations on how the FAA should combat these risks.[76] The GAO report identifies cybersecurity issues regarding NextGen in three main areas: "(1) protecting . . . (ATC) information systems, (2) securing aircraft avionics used to operate and guide aircraft, and (3) clarifying cybersecurity roles and responsibilities among multiple FAA offices."[77]

The ATC information systems require strict cybersecurity protocols in order to ensure the safety of the aircraft.[78] If a malware attack occurs on one of the systems that is interconnected with other onboard systems, the malware could spread, worsening the effects of the attack.[79] An example of this type of issue is if the malware used in the 2008 Spanair attack had first infected an ATC information system and then, through network

---

[71] Jessica Culler, *8 Questions about NextGen, Part 1: How We'll Get Where We're Going Tomorrow*, NASA (Jan. 18, 2012), http://www.nasa.gov/topics/aeronautics/features/8q_nextgen.html; Leighton Quon, LINKEDIN, https://www.linkedin.com/in/leighton-quon-2969015 (last visited Sept. 30, 2016).

[72] Culler, *supra* note 71.

[73] *Id.*

[74] McAllister, *supra* note 65, at 133.

[75] Culler, *supra* note 71.

[76] *See Air Traffic Control: FAA Needs a More Comprehensive Approach to Address Cybersecurity as Agency Transitions to NextGen, GAO-15-370*, U.S. GOVT. ACCOUNTABILITY OFFICE 2 (Apr. 14, 2015), http://www.gao.gov/products/GAO-15-370 (looking at how the FAA has been addressing cybersecurity challenges and making additional recommendations).

[77] *Id.* at 11.

[78] *Id.* at 1.

[79] P.W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR – WHAT EVERYONE NEEDS TO KNOW 43 (2014).

interconnectedness, spread to the central computer system, caused the impairment of other aircraft functions, and ended in a fatal crash.[80]

Although the FAA has made progress in its efforts to protect the ATC systems, it still has not created a cybersecurity threat model.[81] The National Institute of Standards and Technology (NIST) suggested that a cybersecurity threat model be enacted so the FAA can properly determine if there are any threats, no matter how small, to its information systems.[82] Cybersecurity controls should be included as a key part of this model.[83] According to experts, "cybersecurity controls, if properly designed and effectively implemented, can make IP-networked systems more resilient against damage while allowing the systems to interoperate."[84] This model would also help the FAA avoid improperly allocating its limited resources to handle only large cybersecurity threats.[85]

As avionics continue to advance, the stronger the connection between aircrafts and the Internet becomes.[86] According to the GAO report, "[t]his interconnectedness can potentially provide unauthorized remote access to aircraft avionics systems."[87] The potential for large catastrophes due to unauthorized access becomes even more frightening when advanced avionics systems that do many of the tasks usually done manually by pilots, such as

---

[80] Meredith, *supra* note 16 (the 2008 Spanair attack did not involve an infected ATC information system, but the same result could have ensued if it had).

[81] U.S. GOVT. ACCOUNTABILITY OFFICE, *supra* note 76, at "What GAO Found" (no page number provided on this particular page).

[82] *Id.* at 15–16.

[83] *Id.* at 12 (this is because cybersecurity controls help protect IP-networked systems against damage).

[84] *Id.*

[85] *Id.* at 15 (this model could help the FAA "align its cybersecurity efforts and limited resources accordingly to protect its mission," thereby making sure all threats are protected against regardless of size).

[86] *Id.* at 18–19.

[87] U.S. GOVT. ACCOUNTABILITY OFFICE, *supra* note 76, at "What GAO Found" (no page number provided on this particular page).

area navigation (RNAV),[88] are considered.[89] For example, if the RNAV unit is left unsecure, a cyber hacker could remotely hijack a commercial aircraft and use the RNAV unit with autopilot to direct the aircraft to any place it wants.[90] While this is an extreme example, it portrays the grave consequences that can occur if strong cybersecurity measures are not put in place to secure avionics. The FAA has been diligently working to address this type of vulnerability by having its Office of Safety (AVS) take additional steps when completing the aircraft certification process.[91] As one part of the certification process, AVS has to certify that any new interconnected systems abide by the particular rules of that type of aircraft.[92] Also, AVS has started to examine rules regarding the certification of cybersecurity on any new avionics.[93]

One way the FAA has improved the clarity of cybersecurity roles is the development of the Cyber Security Steering Committee (Committee).[94] This committee's purpose is to supervise any type of information sharing.[95] One critical mistake the FAA made in regards to the Committee is that AVS was not made a complete member, and can only be included on an ad-hoc advisory basis.[96] Although AVS may consult the Committee on a case-by-case basis, GAO argues that, "[n]ot including AVS as a full member could hinder FAA's efforts to develop a coordinated, holistic, agency-

---

[88] According to the FAA's Advanced Avionics Handbook, (See Rule 5.1(a)(ii))

> [a] . . . RNAV . . . unit accepts a list of points that define a flight route, and automatically performs most of the course, distance, time, and fuel calculations. Once en route, the . . . RNAV unit can continually track the position of the aircraft with respect to the flight route, and display the course, time, and distance remaining to each point along the planned route. An autopilot is capable of automatically steering the aircraft along the route that has been entered in the . . . RNAV system.

FED. AVIATION ADMIN., ADVANCED AVIONICS HANDBOOK 1–2 (2009).

[89] *Id.* ("Advanced avionics equipment, especially navigation equipment, is subject to internal and external failure. [The pilot] must always be ready to perform manually the equipment functions which are normally accomplished automatically . . . to ensure the flight has a safe ending.").

[90] Doug Gross, *Hacker Says Phone App Could Hijack Plane*, CNN (Apr. 12, 2013), http://www.cnn.com/2013/04/11/tech/mobile/phone-hijack-plane/.

[91] U.S. GOVT. ACCOUNTABILITY OFFICE, *supra* note 76, at 20.

[92] *Id.* at "What GAO Found" (no page number provided on this particular page).

[93] *Id.* at 20.

[94] *Id.* at "What GAO Found" (no page number provided on this particular page).

[95] *Id.*

[96] *Id.*

wide approach to cybersecurity."[97] If it is difficult for one sole government agency to adopt a uniform cybersecurity approach, leaving the agency open to threats, it will be very difficult, yet absolutely critical, to develop an international industry-wide approach to cybersecurity in order to fully protect aviation from these threats.[98]

Aircraft Wi-Fi

Airlines have begun providing wireless network and Wi-Fi access for purchase on board their aircrafts, while still using avionics systems.[99] In the past, avionics guiding and control systems were "isolated and self-contained units" to keep them safe from outside attacks.[100] By using Internet Protocol (IP) networking, a hacker on the ground could possibly gain remote access to, and attack the avionics systems in the cockpit.[101] Traditionally, even though firewalls have been used to protect these systems, firewalls can also be hacked.[102] An example of this would be a person using the on-board entertainment system or the cabin Wi-Fi to access the avionics systems by hacking any firewalls put up as safeguards.[103] According to cybersecurity experts, "if the cabin systems connect to the cockpit avionics systems (e.g., share the same physical wiring harness or router) and use the same networking platform, in this case IP, a user could subvert the firewall and access the cockpit avionics system from the cabin."[104] The FAA has suggested that more security controls for the onboard avionics systems would strengthen cybersecurity.[105]

Not only does Wi-Fi have many of the same security issues as traditionally hard-wired networks, it also brings about a multitude of new issues.[106] One issue that arises for manufacturers is the balance between security and product performance.[107] It is

---

97 U.S. GOVT. ACCOUNTABILITY OFFICE, *supra* note 76, at "What GAO Found" (no page number provided on this particular page).

98 *Id.* at 14–15 (an international and industry-wide approach to cybersecurity is efficient, because problems can be solved quickly, leading to better protection of aviation).

99 *Id.* at 19–20.

100 *Id.* at 18.

101 *Id.*

102 *Id.*

103 U.S. GOVT. ACCOUNTABILITY OFFICE, *supra* note 76, at 18–19.

104 *Id.* at 18.

105 *Id.*

106 MURPHY ET AL., *supra* note 55, at 26.

107 Patrick Cooley, *Government, Cyber Security* [sic] *Experts Raise Concerns*

much easier and cheaper to only have one network on an aircraft, however, as discussed above, one network with firewalls is not a secure enough measure to adequately prevent cyber-attacks on the aircraft.[108] There should always be a separation between public and private networks, such as with Wi-Fi.[109]

Cybersecurity experts warn that "Internet connectivity in the cabin should be considered a direct link between the aircraft and the outside world, which includes potential malicious actors."[110] An aircraft can suffer a cyber-attack through a customer's onboard Wi-Fi usage without them intentionally doing anything wrong.[111] If a passenger visits a website that has a virus, it could allow a hacker to gain access to the "IP-connected onboard information system" through the passenger's now-compromised device.[112] It is not just the passengers' devices using the Wi-Fi that provide the potential for a cyber-attack, pilots or engineers who may bring their personal devices into the cockpit heighten the risk of a cybersecurity breach.[113] Role-based access controls[114] must be put in place to limit the devices that can transmit information, potentially malware, to the avionics systems.[115] According to government cybersecurity investigators, "it is theoretically possible for someone with just a laptop to:

- Commandeer the aircraft
- Put a virus into flight control computers
- Jeopardize the safety of the flight by taking control of computers
- Take over the warning systems or even navigation systems."[116]

Even though these offenses could potentially happen, there are

---

about Wireless Networks on Airplanes, CLEV. (Apr. 23, 2015), http://www.cleveland.com/metro/index.ssf/2015/04/government_cyber_security_expe.html.

108 *Id.*

109 MURPHY ET AL., *supra* note 55, at 26 (for example, "attacks that successfully overcome . . . countermeasures can be isolated to the publicly available network so that they do not infiltrate the airport's private network.").

110 U.S. GOVT. ACCOUNTABILITY OFFICE, *supra* note 76, at 19.

111 *See id.* (discussing general "websites visited by passengers," not specifically websites or people intending to do wrong).

112 *Id.*

113 *Id.* at 20.

114 "Role-based security permissions are based on a user's position or function within an organization." *Id.*

115 *Id.*

116 Matthew Hoye & Rene Marsh, *GAO: Newer Aircraft Vulnerable to Hacking*, CNN (Apr. 14, 2015), http://www.cnn.com/2015/04/14/politics/gao-newer-aircraft-vulnerable-to-hacking/.

systems within the cockpit that would permit the pilot to take over and fix any problems from the attack.[117] By using two completely different networks, it lessens the chances of the private network being infiltrated by malware that could be catastrophic to the company and the systems it uses.[118]

Although none of these types of cyber-attacks have actually occurred, they should not be dismissed, because they are very real threats to the aviation industry.[119] In 2013, a cybersecurity expert confirmed the reality of these types of attacks when he used a smartphone to hack into an aircraft's navigation system and remotely control it.[120] He also showed how a hacker could use the same method to connect to ATC.[121] According to Michael Rundle, a Wired reporter, "[t]hat hack exploited the Automatic Dependent Surveillance-Broadcast navigation system as a way into the rest of the plane's Flight Management System."[122] After this hack, the security vulnerabilities portrayed by the expert were allegedly fixed, but supervised educational hacks, also known as friendly hacks, like this should be done on a continual basis to highlight new vulnerabilities.[123]

A few aviation companies have created cybersecurity-testing programs, similar to supervised educational hacks.[124] United Airlines implemented a friendly hacking program that is limited to its website and mobile applications, not systems like the onboard Wi-Fi or any aircraft control systems.[125] United explicitly warned that if hackers try to break into systems not warranted under the program, the Airline will pursue criminal investigations and civil legal action against the hacker.[126] Under this program, hackers that can break into United Airlines' website and mobile apps, therefore highlighting cybersecurity weaknesses or gaps, will receive between 50,000 to 1,000,000 free frequent flier

---

117 *Id.*

118 MURPHY ET AL., *supra* note 55, at 26.

119 Michael Rundle, *In-flight Wi-Fi is "Direct Link" to Hackers*, WIRED ENT. (Apr. 15, 2015), http://www.wired.co.uk/news/archive/2015-04/15/aeroplane-wifi-hacks-possible.

120 *Id.*

121 *Id.*

122 *Id.*

123 *Id.*

124 Jonathan Vanian, *United Airlines Wants People to Hack Its Websites, Not Its Planes*, FORTUNE (May 14, 2015), http://fortune.com/2015/05/14/united-airlines-hacking-plane/.

125 *Id.*

126 *Id.*

miles.[127] The amount of miles a hacker can receive depends on the size and seriousness of the vulnerabilities.[128] Boeing has also created a friendly hacker program, where it pays specific hackers to try and break into the software used on its 787 Dreamliner.[129] An end to the need for continual aviation cybersecurity testing is unlikely, because it is clear that "many concerns remain within the security world that planes are uniquely vulnerable to hacks."[130]

BASIC CYBERSECURITY FRAMEWORK AND PAST ATTEMPTS AT IMPLEMENTATION OF PLANS

One major cybersecurity policy enforcement problem facing the aviation industry is the unavailability of international cyber governance. The easy, but implausible, solution would be for every country to agree to global uniform policies governing cyberspace, but in today's world that is impossible.[131] For example, laws regarding the kinds of websites citizens are allowed to view and what citizens are allowed to post on the Internet vary vastly by country, so it would be impractical to think all countries would agree to one set of regulations.[132] Although mandatory uniform global cyberspace policies are likely unattainable, the international aviation community should work together to implement standards and best practices for the industry as a whole.[133]

Executive Order 13636: Improving Critical Infrastructure

---

127 *Id.*

128 *Id.*

129 Jonathan Vanian, *How the FAA and Airline Industry Hope to Protect Planes from Hackers*, FORTUNE (June 29, 2015), http://fortune.com/2015/06/29/faa-airlines-planes-hacked/.

130 Rundle, *supra* note 119.

131 *See* MARAS, *supra* note 13, at 140 (discussing barriers like differing cultural norms, views on social issues, and economic situations).

132 *See id.* (discussing cultural and social differences between countries which would impede an agreement to one set of global regulations, such as the fact that the United States provides access to pornographic websites, which violates the cultural norms of Brazil, and protects the freedoms of speech and press for its citizens, whereas Chinese people cannot speak unfavorably about their government without fear of consequences).

133 Juliet Van Wagenen, *Experts Speak to Cyber Security* [sic] *in Aviation*, AVIATION TODAY (June 12, 2015), http://www.aviationtoday.com/the-checklist/Experts-Speak-to-Cyber-Security-in-Aviation_85266.html#.VywhNGZ1Zms.

Cybersecurity

In 2013, President Obama issued Executive Order 13636: Improving Critical Infrastructure Cybersecurity.[134] According to the Department of Homeland Security, this Order was enacted to:

- Develop a technology-neutral voluntary cybersecurity framework
- Promote and incentivize the adoption of cybersecurity practices
- Increase the volume, timeliness and quality of cyber threat information sharing
- Incorporate strong privacy and civil liberties protections into every
- initiative to secure our critical infrastructure
- Explore the use of existing regulation to promote cyber security [sic].[135]

Collaboration between government agencies and the private sector regarding information sharing was emphasized in the Order.[136] There have been mixed reactions as to whether or not the Executive Order provides adequate solutions to enhance cybersecurity.[137]

Proponents of the Order, including members of the private sector, claim that due to the lack of cybersecurity legislation, the initiative is needed to better protect critical infrastructure assets.[138] They also state that the framework has the "ability to alleviate the problems created by a lack of understanding about cybersecurity issues and practices among different classes of stakeholders. . . . [T]he framework provides a common, nontechnical basis for developing consensus on how best to approach cybersecurity needs."[139] Although the Executive Order is only for the United States, its positive aspects, mentioned by its proponents, bring to light features that the international aviation community should consider when developing cybersecurity best practices and frameworks.

Critics argue that the Order does little more than already

---

134 Exec. Order No. 13636, 78 Fed. Reg. 11739 (2013).

135 *Background*, DEP'T OF HOMELAND SECURITY (Mar. 2013), https://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf.

136 MURPHY ET AL., *supra* note 55, at 41.

137 Eric A. Fischer et al., *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress*, CONG. RES. SERV. at "Summary" (Dec. 15, 2014), https://www.fas.org/sgp/crs/misc/R42984.pdf.

138 *Id.* at 1.

139 *Id.* at 18.

existing programs and efforts to create cybersecurity standards.[140] The Order also can be seen as a deterrent for the quick enactment of legislation, because legislators may decide to wait to see how all of the new elements in the Order are implemented and if it is successful.[141] Many opponents of the Order would rather see legislation approved, because laws could speed up the process of creating needed security measures and make cybersecurity standards more concrete.[142] Other issues with the Order are that it either slows down the process of implementing standards or it rushes the development and research of best practices, it is either too intrusive on private actors involved in the critical infrastructure or it is unenforceable on private actors because of its voluntariness, and that the Order's high-risk designation requirement of critical infrastructure entities could result in over-classification or under-inclusion due to the requirement being unclear.[143] The international aviation community will also face these issues, so it must make better standards and processes than the Order did for the United States.

Basic Cybersecurity Framework

In response to Executive Order 13636, NIST created a basic risk-based cybersecurity framework.[144] The framework will act as a collection of industry standards and best practices for organizations to voluntarily use to help control any cybersecurity risks they may face.[145] It is structured to allow for updates and improvements as needed.[146] Although the framework was created by the United States, it relies on successful standards and practices from around the world, furthering its ability to be implemented at an international level.[147] According to the NIST, "[b]y relying on those global standards, guidelines, and practices

---

140 *Id.* at "Summary."
141 *Id.* at 18.
142 *Id.*
143 Fischer et al., *supra* note 135, at 18–19.
144 *Framework for Improving Critical Infrastructure Cybersecurity*, NAT'L INST. OF STANDARDS AND TECH. 1 (Feb. 12, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.
145 *Id.*
146 *Id.* at 2.
147 *Id.* at 3–4.

developed, managed, and updated by industry, the tools and methods available to achieve the Framework outcomes will scale across borders, acknowledge the global nature of cybersecurity risks, and evolve with technological advances and business requirements."[148] The basic cybersecurity framework (Framework)? is made up "of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles."[149]

The Framework Core is a list of cybersecurity activities that the industry has found helpful in controlling cybersecurity risk, which organizations can use to reach specific cybersecurity outcomes.[150] It is made up of five functions (identify, protect, detect, respond, and recover)[151] that happen simultaneously and together produce a "strategic view of the lifecycle of an organization's management of cybersecurity risk."[152] The Framework Implementation Tiers[153] allow an organization to assess the cybersecurity risks it faces and the procedures it currently has in place to handle those risks.[154] A Framework Profile[155] is defined as "the alignment of the Functions, Categories, and Subcategories with the business requirements,

---

[148] *Id.* at 4.

[149] *Id.*

[150] NAT'L INST. OF STANDARDS AND TECH., *supra* note 144, at 7.

[151] NIST defines the five Framework Core functions as:

- Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. . . .
- Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. . . .
- Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. . . .
- Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. . . .
- Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Id. at 8–9.

[152] *Id.* at 4, 8.

[153] *Id.* at 9 ("The Tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe an increasing degree of rigor and sophistication in cybersecurity risk management practices and the extent to which cybersecurity risk management is informed by business needs and is integrated into an organization's overall risk management practices.").

[154] *Id.* at 5.

[155] *Id.* at 11 (according to NIST, "[a] Profile enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities.").

risk tolerance, and resources of the organization."[156] An organization can have a framework profile for each of its cybersecurity activities, creating multiple framework profiles within an entire organization.[157] A profile is useful in highlighting gaps that need to be filled in order to meet risk-management goals.[158]

It is important to note that this basic cybersecurity framework does not replace a cybersecurity program that an organization already has.[159] The framework should be used in addition to the organization's program, which will help strengthen the program and align it with practices used within the aviation industry.[160] For organizations that have not yet established a cybersecurity risk-management program, the Framework can act as a guide in the implementation of one.[161] Overall, this framework is a good starting point for organizations of all size to use in pursuing stronger cybersecurity activities.[162]

Past Attempts by International Organizations to Address Aviation Cybersecurity Threats

International organizations such as ICAO and IATA have been the leading regulatory bodies in international aviation law.[163] Although many conventions and international treaties have been enacted through these organizations, there has not been an adequate international cybersecurity plan implemented for the aviation industry.[164]

ICAO has been the most influential international organization in the development of international aviation cybersecurity practices.[165] At the 12th ICAO Air Navigation Conference (2012),

---

156 NAT'L INST. OF STANDARDS AND TECH., *supra* note 144, at 11.

157 *Id.*

158 *Id.*

159 *Id.* at 4.

160 *Id.*

161 *Id.*

162 NAT'L INST. OF STANDARDS AND TECH., *supra* note 144, at 1 ("The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure.").

163 RONALD I.C. BARTSCH, INTERNATIONAL AVIATION LAW: A PRACTICAL GUIDE 13–14 (Routledge Taylor & Francis Group 2016) (2012).

164 *Id.* (due to problems discussed previously, like differing cultural and social customs and political freedoms enjoyed by citizens of different countries).

165 William Reynish, *Do We Really Need ICAO?*, AVIONICS MAG. (Mar. 1, 2000),

the decision was made to establish ICAO's cybersecurity task force.[166] This task force was assigned to analyze the overall aviation cybersecurity risk and create a "global cyber security [sic] architecture" using input from industry actors.[167] In 2013, ICAO also added the following new Recommended Practice to Annex 17, "[e]ach Contracting State should develop measures in order to protect information and communication technology systems used for civil aviation purposes from interference that may jeopardize the safety of civil aviation."[168] Although this new recommended practice was implemented, ICAO is still working on establishing instructions on what Contracting States need to do to comply with it.[169] Finally, the ICAO Aviation Security Panel has worked on developing cybersecurity policies that address the issues of getting all industry stakeholders to review their cybersecurity methods, pushing States to enact an "aviation security cyber security management plan" to deal with the threats that could unlawfully interfere with civil aviation functions, and deciding which authority is the most appropriate to manage international cybersecurity responsibilities.[170] ICAO is on the right tract, but its efforts to implement international cybersecurity plans have not been thorough or concrete enough, or implemented quickly enough to garner support and address this critical issue.[171]

By executing a three-pronged cybersecurity procedure, IATA has also made an effort to combat cybersecurity risks that airlines are dealing with.[172] This procedure "includes work to understand, define and assess the threats and risk of cyber-attack, advocacy for appropriate regulation and mechanisms for increased cooperation throughout the industry and with and between Governments."[173] Its broadness and generalizations cause this

---

http://www.aviationtoday.com/av/issue/feature/Do-We-Really-Need-ICAO_12581.html.

166 Lim, *supra* note 4, at 85.

167 *Id.*

168 *Id.*

169 *Id.*

170 *Id.* at 85–86.

171 *See Share and Share Alike for Cybersecurity*, IATA (Mar. 8, 2016), http://airlines.iata.org/analysis/share-and-share-alike-for-cybersecurity (discussing generally how efforts to combat cybersecurity threats in aviation are not as mature as in other industries, as well as how there needs to be a greater international consensus to make a recommended cybersecurity practice on a global level a reality).

172 Lim, *supra* note 4, at 86.

173 *Id.*

policy to lack usefulness in solving aviation cybersecurity threats.[174] Even with the downfalls in both ICAO's and IATA's efforts, it is important that they have recognized cybersecurity as a legitimate threat and are working to address it. These organizations cannot solve aviation cybersecurity problems alone, and the entire international aviation community needs to collaborate to develop the best standards to counter cybersecurity risks.

SOLUTIONS TO CYBERSECURITY THREATS

There is no perfect cybersecurity solution, but there are many ways to help alleviate as many threats as possible.[175] It is hard to create one general cybersecurity solution because of uncertainty surrounding continually advancing technology and difficulty in simply defining what cybersecurity encompasses.[176] The best solutions are proactive rather than reactive.[177] Many of the security policies currently in place were established due to past threats.[178] Although learning from previous cyber-attacks and threats is critical, it is just as important to think ahead when creating security policies to help with prevention. Cybersecurity standards are difficult to keep up to date.[179] In reference to cybersecurity standards' difficulty in keeping up with technology, Zodiac Inflight Innovations' company, TriaGnoSys's Managing Director and Vice President of Business Development Connectivity, Axel Jahn, stated, "[w]hat has been established is going to be outdated as soon as you publish it so we need to maybe have a new philosophy on how we are installing things in an

---

174 *See* IATA, *supra* note 171 (discussing that although the policy is intended for airlines, it can be used for airports and ground handlers, among other things, which likely glosses over specific and important cybersecurity points in each part of the airline chain).

175 SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS [sic] IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS 368 (2014).

176 *Id.* at 5–6.

177 Tom LaTourrette & Brian A. Jackson, *Introduction: The Goal of Efficient Security*, *in* EFFICIENT AVIATION SECURITY 3 (RAND Corporation 2012) (strategies are described as "seeming to always be responding to the last observed threat," and, obviously, it would be better to prevent threats and attacks instead of just responding to them).

178 *See Id.* (discussing restrictions on liquids in carry-ons, new imaging devices to see under a person's clothing, and physical swabs and analytic devices used to detect explosive residue, among others, all in response to past threats).

179 *Id.*

aircraft."[180] When new guidelines are created, they must be able to advance as technology advances to keep from always being stuck one step behind.

International Standards

There is a lack of international standards for cybersecurity at airports.[181] According to a survey of airports in the United States, only nine out of twenty-four of the respondents stated that they had implemented a national cybersecurity standard.[182] ICAO is one organization that, if done correctly, could help get multiple nations to agree on international aviation cybersecurity standards.[183] ICAO's Senior Legal Officer, Jiefang Huang, explained that "[b]y joining ICAO, States undertake to collaborate in securing the highest practicable degree of uniformity in regulations, standards, procedures, and organization in all matters in which such uniformity will facilitate and improve air navigation."[184] The need for uniform cybersecurity standards is essential to the international aviation industry, so ideally ICAO should be able to get countries to support this type of international standard.

Passing international standards through ICAO is not as easy as it may seem due to the need for multi-stakeholder governance in cybersecurity.[185] In recent years, ICAO-led initiatives, such as the 2009 Unlawful Interferences Compensation Convention, have struggled to gain industry-wide support.[186] However, some

---

180 Van Wagenen, *supra* note 133.

181 MURPHY ET AL., *supra* note 55, at 41.

182 *Id.*

183 Lim, *supra* note 4, at 85–86 (likely due to ICAO being a specialized agency of the United Nations, thereby having international influence).

184 5 JIEFANG HUANG, AVIATION SAFETY THROUGH THE RULE OF LAW: ICAO'S MECHANISMS AND PRACTICES 45 (Pablo Mendes de Leon ed., 2009); Jiefang Huang, LINKEDIN, https://ca.linkedin.com/in/jiefang-huang-3b6a2947 (last visited Oct. 2, 2016).

185 John E. Savage & Bruce W. McConnell, *Exploring Multi-Stakeholder Internet Governance*, EAST WEST INSTITUTE 3 (Jan. 2015), https://www.eastwest.ngo/sites/default/files/Exploring%20Multi-Stakeholder%20Internet%20Governance_0.pdf.

186 *Convention on Compensation for Damage to Third Parties, Resulting from Acts of Unlawful Interference Involving Aircraft*, ICAO (May 2, 2009), http://www.icao.int/secretariat/legal/List%20of%20Parties/2009_UICC_EN.pdf (this particular convention only received eleven signatures, two ratifications, and four accessions).

industry-led initiatives, such as the 2001 Cape Town Convention, have had greater success at being globally-accepted.[187] This shows that the power of actors within the industry does not lie solely with the government, but with both public and private sector actors. All entities that have an interest in aviation cybersecurity should be allowed to have a say in the creation and execution of international standards, exemplifying the need for multi-stakeholder governance. The Norwegian Institute of International Affairs states, "a 'multistakeholder' [sic] model [is] widely seen as a panacea for securing cyberspace, and the model is employed in several current initiatives in the field of cybersecurity."[188] Not only does multi-stakeholder governance create the likelihood of more support for international standards, it brings together professionals from all areas of the industry that hopefully will be able to discover and address more problems than a single-stakeholder governance would.[189]

One international standard that would alleviate some of the on-board cybersecurity risks posed by the use of Wi-Fi is a cybersecurity airworthiness[190] policy.[191] The Special Conditions[192] issued by the FAA in the aircraft-airworthiness certification process, could serve as a model for the international standard.[193] As of May 2016, the FAA's airworthiness certification did not require cybersecurity to be addressed; however, Special Conditions have been issued to help deal with new cybersecurity problems.[194]

---

[187] *Compare Convention on Compensation for Damage to Third Parties, Resulting from Acts of Unlawful Interference Involving Aircraft*, *supra* note 185 (showing that the 2009 Convention on Compensation for Damage to Third Parties only had eleven signatures), *with Convention on International Interests in Mobile Equipment*, ICAO (Nov. 16, 2001), http://www.icao.int/secretariat/legal/List%20of%20Parties/CapeTown-Conv_EN.pdf (showing that the 2001 Convention on International Interests in Mobile Equipment signed at Cape Town had twenty-eight signatures).

[188] Lilly Pijnenburg Muller, *Securing Cyberspace: Coordinating Public-Private Cooperation*, NORWEGIAN INST. OF INT'L AFFAIRS 1 (2015), https://brage.bibsys.no/xmlui//bitstream/handle/11250/285462/3/NUPI+Policy+Brief-20-15-Muller.pdf.

[189] Savage & McConnell, *supra* note 185, at 3, 10.

[190] U.S. GOVT. ACCOUNTABILITY OFFICE, *supra* note 76, at 20 (when an aircraft is declared "airworthy" it "means the aircraft conforms to its type design and is in a condition for safe operation.").

[191] *Id.*

[192] *Id.* (special conditions are limited-scope rules put on aircraft manufacturers by the FAA "when aircraft employ new technologies where IP interconnectivity could present cybersecurity risks.").

[193] *Id.*

[194] *Id.*

For example, the FAA issued Special Conditions to both Boeing and Airbus in order "to address the increased connectivity among aircraft cockpit and cabin systems for the Boeing 787 and Airbus A350 to provide systems cybersecurity and computer network protection from unauthorized external and internal access."[195] The creation of an international standard insisting aircraft manufacturers around the world provide these types of cybersecurity and IP network protections on any plane, where the interconnectedness of systems could potentially lead to threats, is necessary.[196] Both government actors and industry professionals have expressed support for this type of standard.[197]

The international aviation community should consider enacting an international standard that encourages organizations to use the NIST's basic cybersecurity framework.[198] It was not developed to be a country-specific tool and can work for all-size organizations around the world.[199] NIST asserts, "the Framework can contribute to developing a common language for international cooperation on critical infrastructure cybersecurity."[200] Also, the framework is useful in the aviation industry because organizations can mold it to fit their specific needs for cybersecurity, rather than trying to mold their organization to fit burdensome government regulations.[201] These international standards help guide the international aviation community towards more optimal cybersecurity results.[202]

Information Sharing

Information sharing between all players in the aviation industry is vital to correctly assess vulnerabilities.[203] There are various ways that successful information sharing can be implemented in the aviation industry, one of which is through Information Sharing Analysis Centers (ISACs).[204] ISACs were created in the late 1990s as a way for both public and private entities to share information

---

195 *Id.*
196 U.S. GOVT. ACCOUNTABILITY OFFICE, *supra* note 76, at 20.
197 *Id.* at 15.
198 NAT'L INST. OF STANDARDS AND TECH., *supra* note 144, at 4.
199 *Id.*
200 *Id.*
201 Scott J. Shackelford & Scott Russell, *Above the Cloud: Enhancing Cybersecurity in the Aerospace Sector*, 10 FIU L. REV. 635, 653 (2015).
202 *Id.* at 637.
203 MARAS, *supra* note 13, at 158.
204 Shackelford & Russell, *supra* note 201, at 660.

to minimize cybersecurity threats.[205] One example ISAC is the Aviation Information Sharing and Analysis Center, which businesses involved in the aviation industry can join for a yearly fee ranging from $10,000 to $50,0000.[206] Although this ISAC's information sharing method and strategy is on the right track, there should be collaboration without the imposition of initial membership costs, so that all-size businesses and governments can participate.

As a part of information sharing, there must be public-private partnerships.[207] Executive Order 13636 was supposed to increase information sharing between the public sector and the private sector, but it has not worked as planned due to the policy being voluntary.[208] One suggestion is to make information sharing mandatory, but it would never work on an international level.[209] Not only is there a lack of an enforcement mechanism to make international information sharing mandatory, most countries would never agree to it because of national security risks involved in being required to share certain information with other countries.[210] Each country should encourage private sector actors to participate in information sharing and adopt a framework, by creating helpful mechanisms such as tax incentives, cost sharing initiatives, and example guidelines, to make the process easier to implement.[211] According to Dr. Marie-Helen Maras, "[t]he key to a successful public-private partnership is to enable information sharing without placing an unnecessary burden on the private industry."[212]

International information sharing can be done through already existing organizations like ICAO or as part of alliances formed for this specific purpose.[213] All kinds of alliances can be formed

---

[205] *Id.*

[206] *Frequently Asked Questions*, AVIATION ISAC, http://a-isac.com/ (follow "FAQ" hyperlink, and then follow "What is the cost of membership?" hyperlink) (last visited Oct. 2, 2016).

[207] MARAS, *supra* note 13, at 152.

[208] *Id.* at 156.

[209] *Id.*

[210] *See id.* (additionally, "[c]ompanies may hesitate to participate because they may fear customer backlash, bad publicity, negative attention, and may be reluctant to devote time and resources to implement the standards.").

[211] *Id.*

[212] *Id.*

[213] MARAS, *supra* note 13, at 157 (discussing existing alliances such as the National Cyber-Forensic & Training Alliance and the European Public Private Partnership for Resilience).

between different countries, private sector and public sector actors, and even between companies, such as airlines.[214] An international cybersecurity alliance example is the one that exists between the United States and the European Union,[215] which was established to facilitate information sharing and the further development of cybersecurity best practices.[216] In 2011, this alliance participated in the Cyber Atlantic Exercise[217] that replicated cyber-attacks against both parties' critical infrastructures.[218] The goal of the exercise was to determine how efficiently the United States and the European Union could collaborate and actually put to use the policies of their alliance.[219] International cybersecurity would be greatly strengthened if more alliances were formed and more training exercises were enacted, even if only done within the aviation sector.[220]

Any international standards or best practices that deal with information sharing must address whom the information should be shared with and its confidentiality within the industry.[221] Some people would argue that the public has a right to know about cyber-attacks, but others would rebut this by saying that it is similar to a matter of national security, and that publicizing this information could make things worse.[222] A statement from Airbus addressed this issue, declaring, "Airbus, in partnership with our suppliers, constantly assesses and revisits the system architecture

---

214 *Id.*

215 *Fact Sheet: U.S. – EU Cyber Cooperation*, THE WHITE HOUSE OFF. OF THE PRESS SEC. (Mar. 26, 2014), https://www.whitehouse.gov/the-press-office/2014/03/26/fact-sheet-us-eu-cyber-cooperation.

216 MARAS, *supra* note 13, at 157.

217 *First Joint EU-US Cyber Security* [sic] *Exercise Conducted Today, 3rd Nov. 2011*, EUROPEAN UNION AGENCY FOR NETWORK AND INFO. SEC. (ENISA) (Nov. 3, 2011), https://www.enisa.europa.eu/news/enisa-news/first-joint-eu-us-cyber-security-exercise-conducted-today-3rd-nov.-2011.

218 MARAS, *supra* note 13, at 157.

219 *Id.*

220 *Id.* ("These alliances help develop and disseminate best practices for protecting critical infrastructure and minimizing vulnerability. . . . To prepare for cyber-attacks, countries can conduct cyberincident [sic] exercises.").

221 *See* Jay P. Kesan & Carol M. Hayes, *Creating a "Circle of Trust" to Further Digital Privacy and Cybersecurity Goals*, MICH. ST. L. REV. 1475, 1482 (2014) ("The circle of trust represents our idea that the most pertinent information should be collected into a compendium of vital information that is shared with properly vetted agencies and firms. . . . the participants should not be compelled to share information beyond what is necessary.").

222 *See id.* at 1478–80 (describing generally how cyber-attacks can affect citizens even when aimed at governments, but how governments do not want cyber threat information becoming widely-known).

of our products, with an eye to establishing and maintaining the highest standards of safety and security. Beyond that, we don't discuss design details or safeguards publicly, as such discussion might be counterproductive to security."[223] It would be counterintuitive for anyone involved in private aviation to discuss the security measures in detail, because this information could help hackers break through safeguards.[224] As a part of the international standards, members of the aviation industry need to agree to keep any information, that if released could be detrimental to aviation cybersecurity, confidential.[225]

Training Programs

Every step taken towards strengthening the international aviation industry's cybersecurity is important, no matter how small or insignificant it may seem. Cybersecurity training programs for all aviation organization employees would have a large impact.[226] Different training programs are needed for more telecommunication-involved positions, but by making every employee go through a basic cybersecurity training, it greatly lessens the risk of a threat accessing information via the normally-used employee portals, such as e-mail.[227] Employees must understand how personal devices, such as iPhones, can affect an organization's IP network. Personal devices are sometimes able to get around network security filters and less than a fourth of these devices can be remotely wiped clean of sensitive information.[228] NIST advises "organizations [to] assume that all mobile devices are untrusted unless the organization has properly secured them and monitors their security continuously while in use with enterprise applications or data."[229] It might then seem like a policy banning outside personal devices from the workplace is the safest

---

223 Hoye & Marsh, *supra* note 116.

224 *Id.*

225 *See id.* (discussing that while information sharing is important, the confidential nature of this information needs to be recognized and protected by members of the aviation industry in order to protect against cybersecurity threats).

226 MURPHY ET AL., *supra* note 55, at 2 ("[s]taff are often untrained, resulting in poor habits that expose vulnerabilities.").

227 *Id.* at 13, 19.

228 Lisa Phifer, *BYOD Security Strategies: Balancing BYOD Risks and Rewards*, TECHTARGET (Jan. 2013), http://searchsecurity.techtarget.com/feature/BYOD-security-strategies-Balancing-BYOD-risks-and-rewards.

229 MURPHY ET AL., *supra* note 55, at 31.

solution, but it is unlikely that this policy would always be followed.[230] The organization should create a personal device policy stating the acceptable uses and what company information can be obtained using the device, with a clear line separating personal and work uses.[231] Social media applications on personal devices allow for data leakage and the infiltration of malware into the network, so they should be strictly banned in the personal device policy as well as on any technology connected to the network.[232] The personal device policy is only one layer of security and more methods must be enacted in the likely event an employee violates this policy.[233]

One successful training method example is the cybersecurity education program enacted at Miami International Airport.[234] The Director of Information Systems and Telecommunications, Maurice Jenkins, explained that by simply having all staff take part in educational training sessions where they are educated on how one small mistake, such as clicking on an unknown link in an e-mail, can open up the entire organization to a cybersecurity breach, a decent amount of risk is alleviated.[235] This educational program, combined with upgrading the hardware systems, has significantly decreased the amount of cyber hacking attempts on this airport, that at one point had nearly reached 20,000 attempts per day.[236] Additionally, Jenkins mentioned that his department works with governmental departments and different committees dealing with cyber-attacks and terrorism in order to increase industry awareness of what should and should not be done to combat any potential cyber threats.[237]

Aviation organizations can create their own training procedures using the standards and best practices previously discussed.[238] These organizations can also use specific training tools, such as

---

230 *Id.*
231 *Id.*
232 *Id.* at 33.
233 *Id.* at 32.
234 Danny Palmer, *Education Helps Miami International Airport Reduce Threat of 20,000 Cyber Attacks* [sic] *a Day*, COMPUTING (June 20, 2013), http://www.computing.co.uk/ctg/news/2276385/education-helps-miami-international-airport-reduce-threat-of-20-000-cyber-attacks-a-day.
235 *Id.*
236 *Id.*
237 *Id.*
238 MURPHY ET AL., *supra* note 55, at 61.

the National Cyber Awareness System[239] or PCI-Essentials,[240] which educate employees of all levels on potential threats and the importance of actively following strict cybersecurity policies.[241] These programs can also be set up to deliver alerts to employees when a new threat or new information on how to prevent a cybersecurity breach is obtained.[242]

CONCLUSION

The implementation of cybersecurity frameworks and programs by all members of the international aviation community is critical to maintain the infrastructure and safety of the entire industry.[243] The best solution to cybersecurity problems within aviation is to use international standards, information sharing, and training programs in combination with one another to create a broad safety net for the industry. It is important to maintain these programs with the most up-to-date information and procedures.[244] Cybersecurity programs can create a "false sense of security" among members of the community, so there needs to be ongoing periodic assessments of all tools and people involved in the program.[245] Although it may seem obvious, it is important to keep the cybersecurity program information classified within the industry.[246] There does not need to be any unnecessary attention or publication of these programs because it could prompt hackers to try and penetrate these new security walls.[247] In conclusion, if all international aviation industry actors work together to develop, follow, and continually update international standards, information sharing policies, and training programs, the potential for catastrophic cybersecurity attacks will decrease and industry-wide cybersecurity will strengthen.

---

239 *National Cyber Awareness System*, US-CERT, https://www.us-cert.gov/ncas (last visited Oct. 2, 2016).
240 MURPHY ET AL., *supra* note 55, at 62.
241 *Id.*
242 *Id.*
243 *Id.* at 63.
244 *Id.*
245 *Id.*
246 MURPHY ET AL., *supra* note 55, at 63–64.
247 *Id.*