Critical Infrastructure Project

# The State of Cybersecurity in the Airline Industry

by John Palmer and Michael Markell

# Introduction

The airport is a premier example of where logistical coordination meets hectic business -where a trillion dollar industry meets the necessity of orderly and safe conduct. In that dichotomy, many possibilities for error occur – and where errors occur, business and safety can be sacrificed. It is important to recognize both technical and policy-based decisions that can insure the maximum stability and safety of the airline industry. First, we will discuss specific technical issues which could, unchecked, lead to serious cybersecurity infractions. Thus, management policy, the assurance that the system is run satisfactorily, has become a crucial cybersecurity issue. Furthermore, policy that facilitates adaptation to ever-changing threats is essential in keeping the system safe and smoothly running.

# Part 1: Technical Analysis

## Wireless Network Security

The first issue to be resolved is that of poor wireless network security in airports. While this issue is the least technically complex of the problems being addressed, it is of the utmost importance. In 2008, AirTight Networks performed a test on fourteen airports in the United States, Canada, and Asia, revealing that all fourteen of them were using either open networks or networks that were poorly secured (IJTTE 270). Of the private networks identified, 80 percent of them were using WPE encryption, widely known to be an insecure protocol. While this inadequate level of security is a threat significant enough to warrant technical reform, there also exists the problem of employees' access to airport networks. According to the International Journal for Traffic and Transport Engineering, even in airports with higher levels of network security, employees can connect unapproved devices using their enterprise login credentials. All of this goes to say that airports across the country contain significant technical flaws in the security of their networks.

Although the technical changes that can greatly increase the security of airports are simple, it is important to understand what's at stake so that they can be sufficiently justified. Computer networks are integral to all of the fundamental operations of an airport. They control everything from passenger ticketing to the routing of luggage and other logistical operations. Therefore, a malicious attack on such a network could cause global damage that not only slowed the movement thousands of travelers but also misdirected belongings all over the world. The power to cause these results could do great damage in the wrong hands, posing both a monetary and human threat to the industry.

A few technical recommendations could greatly lower the risk of such an attack. While they are expansive, the changes required to do so are not technically complex. The first of these recommendations is to establish separate networks for critical operations in all airports. Because these new networks will be responsible for the most essential airport logistics, they will need the highest possible degree of security. The most obvious requirement is that these key networks use WPA2 encryption, which, unlike the WEP protocol, changes encryption keys each time a new device connects to the network. This makes cracking the encryption much more difficult for any potential hackers, and the only challenge in its implementation is the potential need for new wireless routers that support WPA2. Another technical specification of these networks is that they should filter access not only by login credentials, but also by the MAC address of any device attempting to connect. The effect of this is that a network will need to know and approve each specific physical device that wants to connect to the network, since each physical device has a unique MAC address. Because these networks are being used to control such important operations, any devices needing to perform these tasks should be identified far in advance, and this technical requirement is a good way to ensure that this happens.

The other side of these technical recommendations is for airport networks involving non-critical operations, such as restaurants and retail vendors. Most airports currently host these tasks on the same network used for critical operations. Even with these things on separate networks, airports must use up-to-date encryption, in this case WPA2, to avoid danger from hackers. This is particularly important because airport employees connect their personal devices to these networks. Additionally, it should be required that employees register their devices that will be connected to the network. This could also be done by filtering wireless access by MAC address, as suggested previously for the critical networks. Once again, the difficulty of enacting such a change is low, only requiring the adjustment of router settings and the regular addition of new approved devices.

## Cyber Operations Database Flaws

Another significant flaw in the technical infrastructure of the airline industry is that of one of its most important event logging systems. All such systems are owned by the National Airspace System, which includes all airports in the United States and has control over all of their related policies, regulations, and information. The NAS contains a Cyber Operations unit (referred to as the NCO), which serves as "the focal point for NAS incident response activities" (GAO 21). However, in a January 2015 report, the Government Accountability Office reported the following:

> The NCO database system containing centralized security logs collected from various NAS systems was ineffective due to weaknesses in its searching function. Specifically, the system could not search past any gaps in the log data. To compensate, NCO personnel would manually parse the data from multiple queries together. (GAO 25)

The magnitude of such a flaw in a database is considerable in this context, and possible consequences could be devastating were this error to occur in a time of emergency. The first and most obvious consequence is that of a delayed response time to an airline emergency. If NCO personnel are required to manually parse through data, it could take far too long to accumulate all necessary information and take action. Another potential problem arises from the fact that even when manually joining queries together, the NCO does not have any guarantee that all necessary information is collected. This means that the NCO could completely miss security logs before and during an emergency. The absence of such logs diminishes the NCO's ability to perform its key task: avoiding and responding to emergencies.

Due to the sensitive nature of specific technical information, the exact type of database system being used by the NCO is not publicly available. However, the problem described is a common result of a poorly constructed SQL database. SQL is a database system that, when implemented properly, can perform extremely efficient searches over billions of data entries. Because the problem being experienced by the NCO is likely part of a SQL database due to its technical nature, recommendations for how to fix it will be described. However, in the case that the NCO database is not built with SQL, these recommendations will still be helpful, as they will inform the NCO on how it can construct a SQL database that doesn't exhibit the current problems with searching.

The GAO reports that the key problem with the event logging system lies within its searching abilities. In the past, when gaps have existed in log data, employees have had to manually join several database queries together, and even then, they have had no guarantee that they received all necessary data. In order to understand why this problem would occur and how to fix it, it is important to understand how a relational database like SQL structures its data, and more specifically how it performs searches.

SQL is a relational database system. This means that within a database, there are many similar kinds of data elements, which are connected to each other via different "relationships." In SQL, a database typically contains several "tables," each of which stores data of the same kind. This is the highest level of organization within a database. Within a table, each data entity is referred to as a row.  A row contains several pieces of information, each of which is called an attribute.  This can be illustrated more clearly with an example.  If an airport wanted to keep track of each flight that departed from its runway, it might make a SQL table to record this. Each row in the table would represent one flight.  Within the row for each flight, attributes might include things like the flight number, destination, airline name, and time of departure for the flight.  Because a table like this contains rows that each contains the same kind of information, SQL can search through the data in a systematic way to look for specific pieces of data that a user wants to find.

However, there's a lot more to a database than just the data it contains.  The actual structure and organization of a database can cause wide-ranging variations in how efficient it becomes to search the data in the system.  Probably the most significant structural decision that a database manager can make is that of adding "indices" on any given table in order to make searching faster.  An index is a tool that helps SQL find relevant data in a much more efficient manner, based on one specific attribute of the rows in the table.  It does this by keeping track of where different pieces of data exist in the table, and storing this information in a separate file that the SQL search optimizer can consult when searching.  This way, when SQL needs to search for data with some specific characteristic, it can save time by looking only in specific locations of the table, rather than searching the entire thing.  For example, if a database manager knew that many users would be searching for departing flights based on time, he could place an index on the "departure time" attribute of the flights table.  The next time a user searched for flights by time, SQL could impose the user's search restrictions on the data and obtain results quickly.

Now that the concept of indices is understood, the NCO's problem can be more intelligently observed. The problem with NCO's system's search functionality only occurs when gaps in its data exist. In other words, if for some range of time, no security events are logged, all logs before that period of time become unsearchable. It is clear that the previous data is not deleted when this happens, just that something about the way the database system is structured prevents SQL from successfully searching in this case. The most likely reason for this is twofold: there is not a proper index placed on the timestamp field of each security log, and there are not sufficient constraints on the data entered into the log table. The result of this is as follows: when NCO personnel need to search for security logs in some range of time, SQL performs a linear, row-by-row search over the security logs due to the lack of an index to inform it how to search more efficiently. However, when SQL performs a linear search in this manner, several different things can cause the search to halt prematurely or exclude important results. For example, if there were some portion of the logs that had a "NULL" value for an attribute on which the table was indexed, the search would stop upon hitting one of these rows. This would exclude from the search results any important data in the table after this row. Additionally if there were some portion of rows in the SQL table for which the only the timestamp value was set to "NULL," these rows would be ignored by the search, although it would continue. If there were important security logs that had somehow been entered to the table without a timestamp, they would be ignored completely by any such searches. This exact occurrence would explain the GAO report from January that states, "there was not sufficient assurance that all data needed for incident investigations had been retrieved" (GAO 25).

Luckily, SQL is a system that can easily adapt to avoid these problems given some technical guidance. The first technical necessity for an event logging system is that the timestamp value of the data entries is indexed. This allows the SQL database to avoid performing a linear search to begin with. In addition, each attribute within the table must be given more strict constraints so that a similar issue doesn't occur in the future. First of all, the timestamp value and any other important attributes must be given the "NOT NULL" specification in the table's declaration. This ensures that no data is entered into the system as a NULL value. While this would help a lot, an even better solution would be to give each attribute an enumeration of possible values. For example, rather than leaving a field like "location" for a security event as an open text value, a specific set of possible locations could be set in SQL as the only values possible for "location." This kind of enumeration would ensure a level of uniformity amongst the rows in a table.

At the heart of the database issues experienced by the NCO is a lack of trustworthy system structure. By enumerating all possible values that can exist in a database, along with placing indexes on the proper values, most of the problems with the NCO's system can likely be avoided. The cost of putting the suggested changes in place is not unreasonably high given the benefits they would bring. Making these technical changes would only cause a one-time delay for the system to be restructured, which should not take more than a couple of days for a database manager.

## ADS-B Radar Weaknesses

A final red flag in current airline infrastructure is the planned implementation of Automatic Dependent Surveillance-Broadcast (ADS-B) system architecture as the radar system in all aircraft, which will be mandatory worldwide in 2020 (Infosec, bottom section). ADS-B systems have been shown to contain security weaknesses in the past, and their usage across the entire industry could introduce glaring vulnerabilities to terrorist attacks . According to a report by Institut Eurécom, “ADS-B protocol used in commercial air-traffic doesn’t specify mechanisms to ensure that protocol messages are authentic, non-replayed or adhere to other security properties” (EURECOM 2). In fact, the same report by Institut Eurécom identified a list of key weaknesses in ADS-B systems, the most important of which are enumerated below:

- Lack of entity authentication to protect against message injection from unauthorized entities.
- Lack of message signatures or authentication codes to protect against tampering of messages or impersonating aircrafts.
- Lack of message encryption to protect against eavesdropping. (EURECOM)

Were a malicious group able to listen to and manipulate aircrafts’ location data or inject false entities into the systems of air traffic controllers, utter chaos could ensue for planes in the air. If air traffic controllers and pilots were unable to discern the positions of other aircraft, consequences could include crashes between planes and multitudes of planes being unable to land. At all costs, this kind of tragedy must be avoided.

The lack of encryption is one of the simpler vulnerabilities to understand. The planned ADS-B system to be implemented in each plane contains two key pieces of hardware that enable it to be in constant communication with other devices. These devices are simply an ADS-B transmitter, which sends data from the plane, and an ADS-B receiver, which can receive messages from other devices. In its current state, the ADS-B system simply sends the required data from one device to another, without any encryption taking place. While this data is sent over a specific radio frequency, and it is highly complex in its nature, all that is required to listen to such data is a commercial off-the-shelf radio receiver, which can be easily purchased. The technical solution here requires very little effort. A layer must be added within the ADS-B system for the encryption and decryption of messages. Doing so would make the observation of flight data by outside parties significantly more difficult.

The other two technical flaws mentioned, vulnerability to injection and manipulation of data, can be addressed together, as they are highly related. Both of these weaknesses stem from the fact that ADS-B systems do not currently employ any form of message authentication. At a high level, what this means is that ADS-B receivers simply listen for any data that is being sent to them. When a message is received, it is processed and relayed to the plane or air traffic tower that it was sent to. However, were an outside group to obtain the ability to send such data, which is not incredibly difficult to do, both planes and air traffic controllers would be left in a position where the integrity of their information was compromised.

While a solution to this problem is more technically difficult, it is absolutely necessary to ensure the safety of passengers in the air. The report by Institut Eurécom proposes one option for doing this, which includes each transmitter sending a signature to its destination bit-by-bit in a complicated manner. While this would be hard to replicate by an attacker, and it is a good possible solution, it could still be cracked by a highly technical group. For this reason, an additional upgrade to ADS-B should be added so that this kind of attack would become nearly impossible. If each ADS-B transmitter is given a unique identification number, the hardware of the transmitter should require that this ID be sent as metadata along with every message the transmitter sends, rather than making it an optional addition. The logic behind this is as follows. If ID's are just sent optionally, a hacker could send a spoofed ID along with any malicious data. However, if the hacker were required to also send the true ID of his/her ADS-B transmitter, the message could be easily identified as a spoof. For this reason, the hardware of each ADS-B transmitter should be built so that its unique identification number is transmitted with each message. The cost of implanting a solution for message authentication in ADS-B systems is certainly non-negligible. Altering the hardware, and thus the manufacturing process for these devices would require costly research and equipment changes. However, given the significance of the technical weakness that is present, such a cost would be justified.

# Part 2: Policy Analysis

The airline industry is currently being revamped and redefined by a series of reforms under the umbrella of Next-Gen, a recent rally of infrastructure and policy reform headed by the Federal Aviation Administration – the FAA. For all the growth that Next-Gen has engendered, it has spawned an array of cyber vulnerabilities as well. Compounding these issues is the unfortunate truth that "there is currently no cyber security standard established for airports in the United States as the existing standards have mainly focused on the Aircraft Control System" (IJTTE, 365). These vulnerabilities necessitate numerous policy decisions, which must be enacted if the entire airline system is to be secure in these rapidly evolving times. Among the issues to be addressed are network security, research goals, insufficient funding of crucial cybersecurity programs, and issues within the FAA's general bureaucratic structure.

## Network Security

Airport networks are one of the most important areas for cybersecurity improvement under Next-Gen. Even small airports are heavily dependent on networked computer systems for daily operations and are therefore vulnerable to cyber threats. As of 2008, 80% of Wi-Fi networks in airports encompassed ticketing systems, baggage systems, shops, and restaurants (IJTTE, 370). Similarly, 23% of airport networks are unsecured, and 80% of secured networks use legacy WEP encryption, a "fatally flawed encryption protocol" (IJTTE, 371). Under Next-Gen, networks are becoming more and more open – more vulnerable to attacks. Although the prior "World War II era" network setup contained significant amounts of isolation, today's networks are far less secure (Goldman). Employees are accessing and exposing this network during the course of their work. Thus, it becomes the job of employees to keep this system secure. To accomplish this, policy must emphasize and train employees to keep the system safe. Although, as per FAA guidelines, employees are updated and retrained every year to be educated on recent cyber policy (FAA Order 1370.106), there are significant holes in the training system. According to the Transportation Research Board, there is a ubiquitous employee trend of "bring your own device," or BYOD. This is an unwise and potentially problematic aspect of the system, and one that needs reform. It is entirely within the potential of this type of system for a major security breach to occur, be it voluntary or accidental, at the hands of an individual employee and their corrupted personal device (GAO).

Thus, a cybersecurity issue with this system is not a farfetched prediction. In 2011, there were 2.9 million hacking attempts at LAX alone (Swan). Although most are stopped, it is very possible for these threats to be realized as action. If, for instance, the baggage system were compromised, baggage could be diverted and skewed for the entire country. The massive delays and confusion could cause resounding effects for the entire industry and the world's economy. Furthermore, mass confusion could have implications for overall airport security – with the massive mobilization of resources to fix such an issue; there would be added confusion to a high stakes industry – one that encompasses 5.4% of the United States GDP. There are several specific policy implementations to rid the network system of these problems. These fixes can be broken up into two categories: structural soundness and employee cybersecurity standards.

One policy based structural fix towards network breaches is that of an organization-wide campaign to convert Wifi networks from WEP to WPA2– a significantly more stable and secure protocol. This addition would not remove the potential for security breach, but it is indeed a prerequisite for network security in this era.

A second specific agenda to be drawn is that of employees – specifically, education and training. Currently, under FAA protocol, employees are trained annually in new cybersecurity standards. However, this training needs reform: not in frequency or scale, or through any new legislation, but in curriculum. Certain standards, such as BYOD, are not conducive to a standard of safety. Thus, emphasis on proper network security standards should be better expressed. One of the most important flaws to fix in the current training system is the notion of a "Top 10" list of permissible employee behavior in cyberspace, the "most common method of education" within the industry (Halsey, Congress).  As Gopalakrishnan notes, this system is problematic in that it gives employees a false sense of security that by doing these ten things, cybersecurity will be assumed. This mindset is problematic - many more than ten potential issues exist within cyberspace. Instead, a specific policy implementation to fix this issue is to develop training curricula that are significantly more extensive and inclusive of all possible issues, covering the entire user layer of interaction (IJTTE, 373). By making the training more comprehensive and avoiding an oversimplification with a "Top 10" list, cybersecurity will be reinforced. These curriculum changes could be mandated by an addendum to FAA Order 1370.106, stating the necessity for revised and improved educational standards pursuant to previously enumerated standards.

Another policy implementation to assure employee cybersecurity is that of device registration. By mandating an organization-wide registration of employee devices, the FAA could counteract the feasible potential for unknown and unsafe devices to enter the network and function as an employee device. In the current system, employee devices need only “enterprise login credentials”, without administrator approval, to access the network. Thus, simply by using an employee’s login credentials, any device - corrupted or not – is allowed access to the network. Through a mandatory policy of administrator approval on a device-by-device basis, these cybersecurity issues can be avoided. As cybersecurity is already a mandatory aspect of FAA employee training, no new legislation is required to realize these training goals: research curriculum is the focus of this change.

## Research Goals

As is noted in the technical section of this paper, the Automatic Dependent Surveillance-Broadcast (ADS-B) system is technically flawed. In order to address the ADS-B system issues and all similar technical issues, there must be logistical coordination and policy-based drive to seek a solution. First, our research suggests the necessity of an implementation of a research team to design an upgraded ADS-B system compliant with the technical recommendations of this paper. Second, upon completion, there will be an initiative led to remove outdated ADS-B system radios, replacing them with the newly created model. Through this mandate, past a specific timeframe, it will be a requirement to use these new devices for all communications with Air Traffic Control. An identical format can be applied for all relevant technical projects, with similar research need. This action could be fulfilled by the introduction of a new FAA order which would mandate the timely switch between the two technologies, in favor of the more recent, secure design. Using the force of mandated legislation, all airports would be required to enact ADS-B improvement.

## Further Considerations

Previously addressed policy decisions were directly aligned with technical decisions made prior in this paper. However, these decisions and implementations are completely contingent upon the most important aspect of policy reform: finance. The problems and solutions for every issue previously discussed are directly related to the raising and spending of capital. In general, the FAA has been inadequately funded. This issue is compounded by the fact that officials inadequately manage the funds that they *are* given (Jackson). These weaknesses are present for a multitude of reasons, and are the topic of this next section, with the goal of adequately financing, researching, and improving upon the airport cybersecurity system. These weaknesses can be broken down into two major categories: lack of awareness of problems, and lack of organization in dealing with these problems.

The first issue to discuss is this lack of recognizing problems. In countless studies, Next-Gen has been exposed as a vulnerable project with countless cyber problems. However, in a personal interview over the phone with the author of this paper, the CIO of a major airline claimed to be "unaware of any cybersecurity issues concerning Next-Gen." This demonstrates a frightful lack of communication between the FAA and the businesses operating airports – especially considering that airlines are the biggest financiers of the entire Next-Gen system overhaul (Broderick). Without knowledge that there are issues with system security, the finances will simply not be raised to deal with cybersecurity issues.

All the while, the issue is compounded by the rapidly changing network infrastructure of Next-Gen, in which years of network security standards are being altered. The CIO's lack of knowledge is a problem, but it is indicative of a greater issue. Airlines, for the majority of Next-Gen planning, were some of the most important financiers. And, although they have poured enormous amounts of money into reform (Broderick), they have recently found uncertainty in the organizations responsible for reform, and have generated less funding (Lowe). Thus, it is the FAA and Next-Gen's job to educate financiers on the needs of their airlines, and the importance of completion, for the consideration of safety. This total lack of cyber vulnerability knowledge by the CIO of a major airline shows an enormous lack of initiative by Next-Gen officials: one that could prove fatal for both the financial and security future of reform. Beyond this lack of confidence from airlines in investment, Congress similarly does not supply the money required to facilitate real growth (Halsey, Congress). Simply put, there is not enough funding to go forward with these plans; there is not enough money for training, awareness and eventual patching of all possible security holes in Next-Gen, which are incredibly numerous and virtually unacknowledged.

The most important issues to manage towards achieving any meaningful reform are not the reforms in and of themselves, but instead, issues of financial moribundity and bureaucratic disorganization. As financial corners are cut, weaknesses arise for the entire system. As (Broderick) states, there is a "chronic" issue with lack of funding for Next-Gen growth. The FAA has repeatedly asked for more currently available funding, and does not have a clear way forward in investment. New funding, the report says, would not necessarily even be a way forward, but a "slow path to recovery," or a way out of the hole that Next-Gen officials have dug (Broderick). Numerous solutions have been proposed, with very contentious battles over which is ultimately selected.

One proposed and highly debated solution for this situation is the bifurcation of the FAA between the bureaucratic mass that it is, and the aspect that maintains air traffic control (Jackson). While well meaning, this step is perhaps infeasible, and most certainly unnecessary. One of the primary justifications for this opinion is the asserted notion that the FAA has "slow decision making and a change-averse culture" (Jackson). Although on some level there is justification for this – difficulty in making milestones, ambiguity in organization, and beyond, this is an unfair categorization. The FAA, although troubled, is severely afflicted by sequestration and congressional uncertainty (Broderick). In essence, these issues boil down to one crucial insufficiency: money. Thus, the issue becomes funding: the who, the how, and the when.

There are two possible ways to increase funding for the Next-Gen system. The first is by finding more capital investment from the United States Government. Since this paper deals with policy action that is feasible, that notion will not be further discussed. Instead, the issue becomes how to incorporate private money, while maintaining legitimacy, and further public goals. Many argue that this is impossible – that private money will inevitably taint the intentions of such an important initiative. However, common sense proves this to be a false dichotomy. First, private industry has already contributed hundreds of millions of dollars to the initiative, so it can't be said that it is, its current state, "pure" (Next-Gen GA Fund). Furthermore, it would be in the airlines' interest to make the system as thorough and secure as possible – it is, indeed, the security of the system that will inevitably determines the level of protection from financial disaster. However, why then would the airline industry refrain from investing enough money into the system to assure a safe and comprehensive program? There are two main reasons, which we will now explore.

The first issue towards gaining private investment is a lack of assurance that Next-Gen is indeed a “safe bet”. This stems, unfortunately, from the problem of money in and of itself. Due to the lack of funding, Next-Gen has been unable to complete many of its milestones. In turn, it has lost much of the legitimacy crucial to its success in raising money (Lowe). The second issue is a lack of urgency and gravity on behalf of the FAA. The organization is plagued primarily by lack of respect for deadlines – Next-Gen, initiated in 2003, is currently calculated to be completed by 2025. Although the very specifics of the FAA bureaucratic mechanism are relatively unknown to a non-credentialed individual, it is nevertheless an obvious assertion that there are issues surrounding deadline urgency which should be of primary concern to the FAA moving forward.

Thus, this paper proposes a cultural reform through institutional makeup in order to eradicate such a crucial institution of these issues. This reform is two-fold: First, there must be clearer communication standards within the FAA so that investors – airlines and the American people, can be aware and willing to show support for increased FAA funding. Second, there must be incentivization of on-time accomplishment of milestones. Let us now dissect these two proposals:

As stated, the FAA has had trouble showing need and garnering support from private industry. Similarly, through issues of sequestration, Congress has hampered much Next-Gen progress (Broderick). Although a true overhaul of the system may be necessary, there are non-legislative solutions that must be explored. In order to gain publicity, popularity, and investor confidence, the FAA should more aggressively comment on ongoing proceedings and difficulties, as well as major successes – of which there have been many. For instance, Next-Gen has saved 4.1 million gallons of fuel and reduced carbon emissions simply due to its work in Dallas alone (Halsey, FAA). By emphasizing and amplifying the responsibility of the press department for the FAA,  of the Next-Gen monetary support may be garnered, and issues would be easier to tackle. It imuchs important to note, here, that this would not require new legislation: rather, it is simple internal bureaucratic change that has control over the realization of this change. Excluding this reform, The FAA's trouble with timelines and managerial style is perhaps more important to discuss, as it inevitably determines the positivity of Next-Gen publicity.

The FAA must incentivize and pressure the implementation of milestones along the path towards a completed Next-Gen system. One potential method for tightening milestones is by creating weekly reports on ongoing projects for managers to oversee: although the fine details of projects may impede objectives, it is then the duty and obligation of the manager to enforce and constrain compliance with deadlines.

Although pressure is one form of incentivization, there are more positive forms of action that could help raise money and ability to accomplish Next-Gen goals. One such methodology is that of tax-credits for cooperative airlines. Although this may be more difficult to accomplish, as it would require new legislative action to be approved for such an act, it would be a surefire way to express to an airline that Next-Gen is a positive investment.

## Policy Conclusions

Policy implementations pertaining to cybersecurity flaws within the airline industry are numerous, but the threat that may be realized as a result of these flaws is unimaginable. Although

Next-Gen is an immense commitment and organizational effort, it is a necessity for the industry and the world as a whole: In the United States, airlines contribute immensely to our GDP, our competitive advantage, and our way of life. It is an obligation to uphold and ensure the integrity of this industry. The costs are high, but the insurance is priceless.

# Works Cited

"Airport Cybersecurity Best Practices." Transportation Research Board. January 1, 2013. Accessed April 9, 2015. http://apps.trb.org/cmsfeed/TRBNetProjectDisplay.asp?ProjectID=3446.

Broderick, Sean. "FAA Budget Request Balances Current Needs, NextGen." FAA Budget Request Balances Current Needs, NextGen. February 5, 2015. Accessed April 9, 2015. http://aviationweek.com/aftermarket-solutions/faa-budget-request-balances-current-needs-nextgen.

Costin, Andrei, and Aurelien Francillon. "Ghost in the Air(Traffic): On Insecurity of ADS-B Protocol and Practical Attacks on ADS-B Devices." EURECOM. January 1, 2012. Accessed April 2, 2015. https://media.blackhat.com/bh-us-12/Briefings/Costin/BH_US_12_Costin_Ghosts_In_Air_WP.pdf.

Cyber Threats against the Aviation Industry." InfoSec Institute. April 8, 2014. Accessed March 17, 2015. http://resources.infosecinstitute.com/cyber-threats-aviation-industry/.

"FAA Needs to Address Weaknesses in Air Traffic Control Systems." United States Government Accountability Office. January 29, 2015. Accessed March 12, 2015. http://www.gao.gov/assets/670/668931.pdf.

"FAA Order 1370.106." June 16, 2009. Accessed April 9, 2015. http://www.faa.gov/documentLibrary/media/Order/1370.106.pdf.

Goldman, Jeff. "Security Flaws Found in U.S. Air Traffic Control System." ESecurity Planet. March 4, 2015. Accessed March 13, 2015.

http://www.esecurityplanet.com/network-security/security-flaws-found-in-u.s.-air-traffic-control-system.html.

Gopalakrishnan, Kasthurirangan, Manimaran Govindarasu, and Doug W. Jacobson. "Cyber Security for Airports." *International Journal for Traffic and Transport Engineering* 4, no. 3 (2013): 365-76. Accessed March 16, 2015. http://www.ijtte.com/uploads/2013-12-30/5ebd908d-7f47-e96dIJTTE_Vol 3(4)_2.pdf.

Halsey III, Ashley. "Congress Considers Privatizing the Air Traffic Control System." Washington Post. March 24, 2015. Accessed April 9, 2015. http://www.washingtonpost.com/local/trafficandcommuting/congress-considers-privatizing-the-air-traffic-control-system/2015/03/24/b63a38f4-d23d-11e4-8fce-3941fc548f1c_story.html.

Halsey III, Ashley. "FAA Rolls out Taste of NextGen in Dallas." Washington Post. November 19, 2014. Accessed April 9, 2015. http://www.washingtonpost.com/local/trafficandcommuting/faa-rolls-out-taste-of-nextgen-in-dallas/2014/11/19/13a5210e-7017-11e4-893f-86bd390a3340_story.html.

Jackson, William. "What's Keeping FAA's NextGen Air Traffic Control on the Runway? -- GCN." What's Keeping FAA's NextGen Air Traffic Control on the Runway? -- GCN. July 22, 2013. Accessed April 9, 2015.

Lowe, Paul. "Stakeholders Debate NextGen Funding Options." Aviation International News. June 5, 2014. Accessed April 9, 2015. http://www.ainonline.com/aviation-news/aviation-international-news/2014-06-05/stakeholders-debate-nextgen-funding-options.

"Next-Gen GA Fund." NextGenFund. January 1, 2014. Accessed April 9, 2015. http://www.nextgenfund.com/files/downloads/NextGen GA Fund Web Release.pdf.

Swan, Darin. "Assessing Primary Cyber Threats to an International Airport's Critical Information Systems." Assessing Primary Cyber Threats to an International Airport's Critical Information Systems. Accessed April 9, 2015. http://www.academia.edu/1460287/Assessing_Primary_Cyber_Threats_to_an_International_Airport_s_Critical_Information_Systems.