Evaluating the impact of NextGen's air traffic system on aviation security

LV Weiland*, and G Wei

Embry Riddle Aeronautical University, USA

Abstract. Networked Next Generation Air Transportation System (NextGen) opened the gate to digital National Airspace System (NAS) in cyberspace. Air traffic improvements from NextGen system, accompanied by the risk of long-standing cyberattack issue in information technology industry became an increasingly challenging matter to the aviation community and Air Traffic Management (ATM), as cybersecurity challenges in the NextGen system could affect NextGen's principle assurance of safety and security in air transportation. The technological shift of NAS infrastructure from traditional radar-based systems to networking system of systems leads to a review, revision and redefinition of current policies, standards regulations, cultures and norm to reflect and mitigate new risks. Through analysing reports, regulations, standards, practices, recommendations from government and industry, the researchers analyse security impacts to NextGen; the risk of a cybersecurity incidents; and regulations to identify most effective and efficient control measures over information systems in ATM, and direction to further research.

1 Introduction

A question raised from incidents is, how do we prevent cyber-attacks in ATM? Before looking for the answer, another question should be answered first. What have we done to prevent cyber-attacks in ATM? NextGen information systems (IS), not only creates billions dollars in economic value and millions of job opportunities like other industries [1], but it also has distinctive and immediate impact on the NAS security and public safety, as it provides safe and accurate air communication in a complex environment. Upgrade to network-based IS in aviation concerns security, safety, aircraft design research, aviation regulations, and training certification in both government and private sectors. Understanding development status, limitations, and responsibilities of each part will better position aviation for approaching aviation cybersecurity.

2 NextGen in the U.S. National Airspace System (NAS)

2.1 Network Construction

* Corresponding author: weila8f3@erau.edu

Interconnections of physical components using network technology, Information Systems (IS), hardware and software created a NextGen net-centricity environment to share aeronautical data “timely and seamlessly among users, applications, and platforms” [2]. Based on FAA official website data, information from FAA Telecommunications Infrastructure (FTI) Overview [3, 4, &5], the fundamental infrastructure enabling net centric operations is System Wide Information Management (SWIM) built upon Federal Telecommunications Infrastructure.

2.2 Threats

2.2.1 Characteristics

U.S. Government Accountability Office (GAO) [2] described cyberattacks as “evolving, growing”, “intentional or unintentional” (p. 1), and cyber-based or physically damaging adversaries against NextGen system with various sources. Testimonies [6, 7] further revealed that criminal groups, hackers, insiders, other nations, and terrorists had been the primary actors of cyber threat based on government and nongovernment data. Leaders of National Business Aviation Association (NBAA) and American Association of Airport Executives (AAAE) stated insiders’ threat was the biggest issue of cybersecurity [8].

2.2.2 Methods

GAO report [6] and testimony [7] also revealed more than 20 methods and exploits of cyberattacks commonly used against federal systems, and among some of them were uncommonly known to the public. For example, creating fake wireless internet access point in public, such as coffee shops, to collect information of victims frequently visited websites, and injected malware to websites to attack targets (watering hole), driving in targeted areas with wireless capability equipped computers to search for unsecured network (war driving), or transmitting more data than system could handle resulting in deletion of data or execution of malware (buffer overflow). Based on target of the attack, threats can be classified as direct, indirect, and human.

2.2.3 Science of modern communication

The core of NextGen is the integration of numerous NAS IS platforms using digital communication technology wirelessly or wired. Wireless communication IS, such as Data Comm, SBSS, AatS, and ACARS transmits on-and-off electrical signal using modulated radio wave or microwave at a frequency ranging from 30 MHz to 3000GHz within electromagnetic (EM) spectrum [8, 9]. The client is an application or interface allowing users to access servers to create, change or delete data. Some client interfaces allow users to make a critical change to the IS depending on protocol and level of authorization. In the context of NextGen IS, which consist of both wired and wireless network channels in many physical facilities such as airports, ATC towers, ground stations, and air routes in space, access to encrypted and modulated signals from authorized or unauthorized devices, systems or computers could be everywhere.

2.2.4 Culture artifacts

Motivations behind unauthorized access to NextGen IS varies. Not understanding these motivations resulting in "prematurely reactive" threat response [10]. State-sponsored

attacks and terrorist attacks call for immediate actions of both private and government efforts with thorough preparation, while random phishing emails could be mitigated through in-house training, education, and continuous monitor. Motivations of threat actors could be divided into 6 categories: curiosity, revenge, revelation, espionage, destruction, and money.

2.2.5 NextGen cyber issues

GAO report [5] stated FAA heavily relied on a huge network of hardware, software, and communication equipment including over 100 different systems to function properly. The agency showed weaknesses in user access control to its systems, control of network system, software and device change and update, uncompleted agency-wide information security program required by Federal Information Security Management Act of 2002, improper governance structure and practice in accordance with National Institute of Standards and Technology guidance (NIST), and ineffective response to and detection of cyber issue. Another GAO report [4] revealed that both FAA and security experts acknowledged avionics systems onboard aircraft could be accessed and planted in with virus or malware from inside and outside of the airplane through in-flight Internet Protocol (IP) based network; and FAA accepted security control of NextGen system provided by its contractors without evaluation and oversight on the matter. Another research showed that SBSS network was also subject to the same cyber threats [11]. Furthermore, ADS-series, ADS-based systems such as CPDLC, WAM, TCAS, FIS-B, TIS-B, radar-based navigation aids systems such as PSR, SSR, GPS, VHF VOR, ILS, NDB and DME, are subject to jamming denial of service, spoofing, and authentication issue [12]. Though impact on confidentiality, integrity, and availability of aeronautic information due to technology or systemic vulnerability could be minor, however, the aviation industry is subject to another more severe threat: human aspect.

3 Government

3.1 Presidential Policy Directive (PPD) 41

3.1.1 Summary

Former Obama signed Presidential Policy Directive (PPD) 41 on 26 July, 2016 to form the Cyber Unified Coordination Group (UCG) to handle significant cyber incidents which were “likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people” [13]. The three agencies will coordinate closely to detect, protect and recover from significant cyber incidents involving federal government system unless such incidents affect private entities, in which case, the relevant sector-specific agencies would coordinate federal government recourse to determine response action [12].

3.2 Federal Aviation Administration (FAA) and cybersecurity

3.2.1 Organizational

Under current FAA structure, five offices and one committee would be responsible for cybersecurity [4]. GAO [4] discovered cybersecurity responsibilities within the agency were not clearly identified and clarified. Additionally, the FAA did not fulfil its external cybersecurity responsibilities established by Department of Transportation (DOT) [14]. Despite this requirement, DOT was not aware of any cyber incidents which FAA reported directly to DHS since the deployment of NextGen; and it did not have access to NextGen air transportation information, or receive any request from the FAA to change or monitor the system; critically, DOT discovered issue of partially monitoring of NAS which was previously identified by GAO in early 2015 [14]; [4]. The increasing demand for cybersecurity, which would play a determining role in maintaining continuity of NextGen operation, inside FAA could affect its performance. FAA has been relying on its inspectors and National Transportation Safety Board (NTSB) to provide safety guidance and regulation over civil aviation in the physical world. Reports from the GAO and DOT provided evidence to show FAA could only observe cybersecurity matters in its traditional safety mind set not from a security perspective.

4 Cybersecurity vs safety culture

As governing body of aviation and safety, FAA [1] has been emphasizing the foster of positive safety culture (PSC). However, does PSC effectively help FAA to address challenges of cybersecurity? PSC has five aspects of culture: informed, reporting, just, learning, and flexible [15]. Informed culture addresses IS administrators as having knowledge of system/s in various aspect to determine safety readiness; and reporting culture refers to people' readiness in an organization to report incident or accidents. FAA has failed on these two aspects both externally and internally [14]. Poor reporting culture resulted in poorly informed culture. Years of partial system monitor show the lack of practical cybersecurity guidelines. During the audit OIG saw a mitigation plan developed. The audit report showed FAA's lack of just culture, with an atmosphere that did not lead to people understanding the difference between acceptable and unacceptable behaviour and the promotion of acceptable behaviour. The FAA failed to develop a required Plan of Action and Milestone (POA&M) as per DOT Cybersecurity Compendium to resolve 273 cybersecurity incidents [16]. The FAA has a learning culture, an organizational climate that encourages continuous improvement, but was not evident in its response to the known issues as it was found to repeat some of the same cyber issues [4; 5; 14]. Good learning culture not only includes active response to known issues but also embraces proactive effort to improve the system as a whole. Flexibility culture in FAA was positive as the agency allocated multidepartment's resource to confront challenges, for example, creating ARAC to address NextGen cybersecurity. At this point, FAA's actions, and behaviours did not "demonstrate a commitment to safety over competing goals and demand" [1, p 11]. However, drawing the conclusion of positive safety culture in the context of cybersecurity during the development of the cyber system is premature as the foster of culture takes time, especially, in the case when established cultural experience has a challenge of new risks.

5 Airline and airport cyber development

Before NextGen network-based IS has been in place in airports and airlines. Thus, they both have some levels of cybersecurity ownership. How each develops future information technology (IT) will affect integrity and security of NextGen systems as airports provide critical and physical entrant to the NAS.

5.1 Airlines

SITA [17], a major worldwide telecommunication and IT service provider to air transportation industry, has been conducting annual airline IT trends for years. Its latest report revealed airline fleet aircraft have and will continue to become more connected with internet using new systems. In cybersecurity, more airline board-level executives and management are assuming responsibility. About 25% of airlines were prepared for cyberattack and 70% airlines had strengthened cybersecurity education and training. These data were based on a survey of the 200 top airlines worldwide of which 14% represented airline from the Americas [17].

5.2 Airports

SITA also followed airports and investment in PED based service such as a mobile purchase at an airport and saw increases of service needed [18]. Airports also began to implement IT, for example, cloud services and sensors to improve operation efficiency. However, more than 40% of airports were still developing cybersecurity strategy, and only 19% were prepared for a cyber-attack [18].

5.3 Report Analysis

Both reports provided IT development trends in the global market. It did not provide specific details of US airlines and airports. Additionally, though airlines showed support for cybersecurity training and educations, evaluations of cybersecurity efficiency were not present. Effective cyber training and education alone will not guarantee effective cybersecurity measures, but would move towards hardening the systems. Also, resources to invest in IT and develop cybersecurity strategy varies among airlines and airports depending on finance and skills the organizations possess, resulting in a different level of understanding and preparedness of cybersecurity [17;18].

6 Challenges

This research identified multiple challenges. First, FAA's lack of effectiveness and efficiency in addressing aviation safety due to cyber issues to fulfil its responsibilities during NextGen's implementation in long term. Before the intention and method of attack could be determined by DHS, as directed by PPD-41, FAA was not being able to identify the cause of an issue, nor direction to approach solution while other aircraft having the same design would remain under risk. Second, is the increasing dependence on integrated and automated IS requiring FAA to monitor and maintain NextGen. For example, malfunction or replacement of SBSS components. Comparing automobiles relying on GPS for navigation on an interstate highway where separation is small, any GPS malfunction could result in automobile crashes, and the risk would be high. The third challenge, shortage of cybersecurity talents. As the aviation industry would become more and more connected with internet, it would demand investment in cybersecurity. Morgan [19] estimates the US shortage of cybersecurity employees in the thousands. The fourth was effective monitoring and intelligence collection for positive cybersecurity without intruding privacy. Cybersecurity would necessitate a large amount of monitoring, such as monitoring employees to comply with policies, IS configuration, internet usages, and passengers' behaviours, and collecting personal information from the internet to determine a level of risk. Privacy would become a more sensitive matter as consumers are exposed more to the internet. The fifth was cybersecurity requirement without regulation for airports and airlines. Airports and airlines have approached cybersecurity differently based on their own

situations. Cyber-attacks occur at weaknesses which have the least amount of difficulty and resistance. Once one system is compromised, other systems are potential victims. Thus, airlines and airports have shared cyber risk and cyber responsibility. However, lack of regulations would result in different approaches and standards. Last, the growing numbers and evolving techniques of cyber-attacks from various sources. Continuous investment, education, training, and learning is required; however, the outcome of such effort is not promising in a complex environment consisting of both cyber and physical worlds.

7 Recommendations

7.1 Countermeasure redefined

Understanding of issues and identification of challenges would better prepare the airline industry for developing solutions that would encompass conceptual ideas of objectives and methods. The word cybersecurity has been used commonly on the internet as a countermeasure against cyber-attacks and cyber threats. Federal government defined cybersecurity as: Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure [20]. This definition manifests every aspect of actions and activities related to cybersecurity which could apply to the aviation industry on an organizational scale instead of global infrastructure scale.

7.1.1 Approach

Different activities have a different level of impact on cybersecurity. Proactive activities such as threat and vulnerability reduction would lead to a direct positive outcome, while the effect of incident response and recovery policies would not be seen until an incident occurs, and it improves an organizations' experience. This difference of impact causes organizations to emphasize policies and activities deemed to be effective based on their knowledge, skills, resources, risk, and priority.

7.1.2 Holistic

Keanini, Chief Technology Officer of Lancop Inc, network security analytic service provider owned by American networking hardware company Cisco, said holistic approach was based on decision-making theory of OODA Loop [21], created by military strategist and former U.S. Air Force Colonel John Boyd. The holistic approach is a comprehensive and continuous process to address cybersecurity by using OODA loop consisting of observation, orientation, decision, and action. The holistic approach calls for operating OODA loop at faster pace continuously than threat actors to increase resistance to threat and raise expenses for threat actors while strengthening cybersecurity. NIST and other security experts also recognized that this approach would allow an organization to develop a comprehensive understanding of threats against IS and level of risk [4]; however, they acknowledged this approach is “costly and time-consuming” (p. 17).

7.1.3 Offensive

Paganini [22] discussed offensive approach involves attribution and retribution; attribution referred to any effort to hunt for and track threat actors and retribution was retaliating action following identification of threat actors. He further pointed out attribution was achieved using a series of aggressive techniques, such as intrusive malware, malicious code, massive-area wiretapping, monitoring, and spying, and that organization damaged or monitored threat actors' system using guaranteed sophisticated methods like zero-day vulnerabilities. This approach, however, came with ethical and legal issues as it threatened privacy. Spying and monitoring have become so easy through commonly used smartphones and applications. Remaining unknown to many, companies have been tracking location history, recording conversations, and monitoring internet usage along with face recognition, for the purpose claimed to be marketing research [23]. Another concern is offensive approach would increase the market demand for zero-day vulnerabilities. Fundamentally, this could encourage hackers and other cyber talents to research, test, and develop more vulnerabilities and exploits to satisfy the market need. Many exploits have been open-source and free for use, potentially it increases cyber threat.

7.1.4 Risk based

National Institute of Standards and Technology (NIST) [24] developed and updated a risk-based framework to demonstrate a common process of cybersecurity implementation led by organization senior executive and top management. The framework consists of five core elements, four implementation tiers, and profile. Five core elements are to identify, protect, detect, respond and recover to threats. Implementation tiers, used to describe the level of preparation, includes partial, risk-informed, repeatable, and adaptive. At last, profile refers to the level of achievement in terms of established objectives such as current or target profile. Top managers and senior executives make a cybersecurity profile based on priorities, risk assessment and decisions, middle-level managers allocate organization resources to implement the profile. Businesses would adapt to this approach easily. However, positive outcome relies on senior executive level's skills, experiences, and expertise to make the right priority and decision once the profile is implemented.

7.2 International movement

International Civil Aviation Organization (ICAO), International Air Transport Association (IATA), Airports Council International (ACI), Civil Air Navigation Services Organization (CANSO), and International Coordination Council of Aerospace Industries Association (ICCAIA) have been taking joint action to address cyber treats in all levels since 2014; Civil Aviation Cybersecurity Action Plan was signed in effect to align with 27000 series standard of International Organization for Standardization and NIST, which was the risk-based approach [25]. Moreover, 39th Session of ICAO Assembly recommended cybersecurity regulation suggesting best standards and practices [26]. ISO 27000 series have established requirements, guidelines and general principles to implement the information security management system (ISMS); specifically, the ISO 27005 has provided guidelines and process for organization information security risk management to assess, treat, and monitor risk [27]. Guidelines and processed are available. Global concurrence and participation is needed

7.3 Best Practice

At this point, research found previously mentioned approaches and standard did not provide effective and specific methodology, except the overall processes and areas of actions encompassed in the definition of cybersecurity. Looking at the matter from standpoint of aircraft operating environments and challenges, no best standards or practices is hack-proof. Best practices of cybersecurity should be systems that organizations periodically and continuously review every cybersecurity matter to identify, assess, treat, and improve risk of cyber threats involving effort of executives, managements and employees and adapt to change so that organizations remain strategically competent in an evolving and complicated digital environment. Cyber threat, cyberattack, and cybersecurity is not a war between digital machines, but it is the war between humans. Human resource is the best tool every organization can have. And the best practice is to reduce, or eliminate threat from insider, and better equip employees and management with reliable information, effective training, and efficient resources.

7.4 Management and cybersecurity

Before any regulation is put in effect, aviation service providers (non-federal) set their own standards and practices of cybersecurity. Though statistics showed low level cyberattacks with limited impact, risk of catastrophic attacks remained as they were difficult to detect [26]. Therefore, it is imperative for organization executives to have a holistic and realistic observation of risk, challenges and assets before establishing cybersecurity program. Incorporation of cybersecurity program which requires monitoring of employees' activities is also a critical challenge for leadership of executives and managements who depend on an effective team of employees to achieve organizational goal. Efficiency to incorporate cybersecurity program in aviation organization would further justify whether executives and managements possess great leadership to influence their employees to accept being monitored to achieve organizational cybersecurity; most importantly, complying with or institutionalizing cybersecurity would have direct impact on cybersecurity readiness [27]. Compliance is to put a program into action, and contrarily, institutionalization is to foster culture, custom and atmosphere of cybersecurity throughout the organization to achieve maximum level of cybersecurity readiness with all-hand participation. Without institutionalization of cybersecurity, even the most secured systems would be exposed to cyber threat induced by humans.

8 Conclusion

Finally, this research found that, beginning its long-term implementation and development, fundamental shift to advanced technology based NextGen NAS had caused numerous gaps and introduced a significant amount of impact to the transportation industry, which could be potentially tragic to aviation security and public safety in the context of cybersecurity. These gap involves legislation, regulations, industry culture and customer, standards and policies in governments and agencies from both federal and states, aircraft and parts manufacturers, suppliers and customers, airline operators, pilots, aircrews, ground personals, contractors, and other related service providers; and it required aviation industry immediate actions to shorten the gap before disaster strikes in the NextGen system of systems for air traffic management. Positive cybersecurity outcome rests on aviation to develop shared vision, responsibility, intelligence, and resources, to institutionalize standardized circle of cybersecurity, and to fight cybersecurity as united entity. Four directions of further research were also identified during this research: effect of regulating minimum cybersecurity requirement on outcome of incorporating cybersecurity program in private sector, effective institutionalization of cybersecurity in airlines and airport, effective approach for airlines to

ensure integrity and security of avionics and IS on-board aircraft, and individual minimum level of cybersecurity education and training in terms of assigned role and responsibility.

References

1. U.S. Federal Aviation Administration (FAA) 2016 (Website) *Safety management system* Order 8000.369B
2. U.S. Department of Defence DoD) (Website) 2007 Data sharing in a net-centric Department of Defence DoD Directive 8320.02
3. FAA 2015 FTI overview [PDF slide document]
4. U.S. Government Accountability Office (GAO) (Website) 2015a *Air traffic control - FAA needs a more comprehensive approach to address cybersecurity as agency transitions to NextGen* (GAO-15-370).
5. U.S. GAO (Website) 2015b *Information security: FAA needs to address weaknesses in air traffic control systems* (15-221).
6. Cybersecurity: Actions needed to address challenges facing federal systems: Testimony before the Committee on Oversight and Government Reform, House of Representatives, GAO-15-573T 2015 (testimony of Gregory C. Wilshusen) (Website) 2015
7. [14] National Telecommunications and Information Administration Office of Spectrum Management 2010 NTIA (website)
8. Combs P 2014 *Top five security topics raised at aviation security summit. NBAA Flight Plan* [Audio podcast] (Website)
9. Gallager R 2006 *6.450 principles of digital communications I* [course materials] (Website)
10. Grimes R 2011 Your guide to the seven types of malicious hackers Infor World (Website)
11. Wood R 2009 *A security analysis of the data communications network proposed in the NextGen air traffic control system* (OSU Website)
12. Stromeler M Schafer M Pinheiro R Lenders V Martinovic I 2016 On perception and reality in wireless air traffic communication security IEEE Transactions on Intelligent Transportation Systems 1-20 doi 10.1109/tits.2016.2612584
13. Office of Inspector General 2016 *DOT cybersecurity incident handling and reporting is ineffective and incomplete* (FI-2017-001) (Website)
14. Cilluffo F & Cardash S 2016, July Overview and analysis of PPD-41: US cyber incident coordination [Web log post]
15. Reason J 1997 *Managing the risks of organizational accidents* Ashgate
16. Office of Inspector General 2017 Audit report (AV2017020) (Website DoT)
17. SITA 2016a Airline IT trends survey (Website)
18. SITA 2016b Airport IT trends survey (Website)
19. Morgan S 2016, Jan. One million cybersecurity job openings in 2016. Forbes.m
20. U.S. Executive Office of the President 2009 *Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure* (DHS Website)
21. Keanini T 2014 *The ooda loop: A holistic approach to cyber security* [Video file]

22. Paganini P 2013 The offensive approach to cyber security in government and private industry. InfoSec Institute (Website)
23. Hern A 2015 *Six ways your tech is spying on you – and how to turn it off* The Guardian (Website)
24. National Institute of Standards and Technology 2017 Framework for improving critical infrastructure cybersecurity NIST (Website)
25. International Coordinating Council of Aerospace Industries Associations 2016 *Coordinating cybersecurity work* In 39th Session of ICAO Assembly (Website)
26. International Civil Aviation Organization (ICAO) 2016 *Civil aviation cyber-security: Possible actions by regulators and stakeholders* In 39th Session of International Civil Aviation Organization (ICAO) (Website)
27. Civil Air Navigation Services Organization (CANSO) 2014 *Canso cyber security and risk assessment guide* (Website)