EMBRY-RIDDLE
Aeronautical University
SCHOLARLY COMMONS

International Journal of Aviation, Aeronautics, and Aerospace

Volume 6 | Issue 1 Article 9

2019

MRO Cybersecurity SWOT

Danita Baghdasarin
Boeing, baghdasd@my.erau.edu

Scholarly Commons Citation
Baghdasarin, D. (2019). MRO Cybersecurity SWOT. *International Journal of Aviation, Aeronautics, and Aerospace, 6*(1). https://doi.org/10.15394/ijaaa.2019.1318

Introduction

The term *cybersecurity* is subjective and its definition continues to evolve with the advancement of modern technology. Cybersecurity is often associated with complex technology and malicious manifestations of security breach. Often overlooked are the human and process aspects of security assurance and the possibility of accidental security breach or security oversight. Craigen, Diakun-Thibault, and Purse (2014) provided a comprehensive and adaptable definition of cybersecurity, which accounts for the various interrelated aspects of the process, stating "cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign *de jure* from *de facto* property rights" (p. 17). This definition describes a threat-management process in which infrastructure, including people and policy, are used to defend against unauthorized access or change to cyberspace or the information stored therein.

The concept of cyber-crime, which includes cyber-attacks and cyber terrorism, is terrifying for several reasons. Technology is everywhere, from personal homes and vehicles to the workplace and public space, and is interacted with constantly. Cyber criminals have copious opportunities to commit crimes, with the advantages of doing so anonymously and at a low cost (Abeyratne, 2011). McAfee identified ransomware as the fastest growing cybercrime; it costs approximately $200 to install, but has a staggering impact to both individuals and corporations (2018, p. 11). The Federal Bureau of Investigation reported $24 million in ransom payments in 2015, which increased to $209 million in just the first quarter of 2016. Altogether, the global cost of cyber-crime was forecasted to reach $600 billion in 2018, almost double the amount estimated in 2014 (McAfee, 2018, p. 6). As aviation is an industry that is becoming increasingly technology-dependent, safety and security professionals must take special care to identify cyber risks and put appropriate mitigations in place.

Cybersecurity in Aviation

The importance of cybersecurity is recognized by the International Civil Aviation Organization (ICAO), which explains that aviation is complex and integrated by nature and therefore relies highly on electronic communications and information storage and sharing, making it a tempting target for the growing threats of data theft. ICAO (2016) called for international collaboration and coordination in the form of media and initiatives to communicate cybersecurity issues and unified strategies for addressing them. Specific objectives included

- identification and classification of threats and risks and the systems they may affect;
- establishment and communication of regulatory and industry stakeholder responsibility;
- communication of known threats and risks and writing of policy to address them; and
- development of a global cybersecurity culture (ICAO, 2016).

Cybersecurity issues, according to ICAO (2016), can be addressed via the safety management system (SMS). In the United States, the Department of Homeland Security considers the following to be six important areas of aviation to watch for risk: global positioning systems, operations and information technology infrastructure, air traffic control, wireless networks, maintenance, and *other unknown threats* (Higgins, 2017).

Aviation Maintenance

Within aviation, the maintenance, repair, and overhaul (MRO) industry seems particularly weak in its preparedness to handle cybersecurity issues. The network of original equipment manufacturers (OEMs), airlines, and airports is large, and the supply chain consists of many opportunities for a cyber-criminal to slip in undetected, especially when the target is a smaller and less cybersecurity-savvy organization. MROs are particularly vulnerable to supply chain attacks due to their around-the-clock operations, global reach, and the lack of international standardization in cybersecurity assurance (Costanza & Prentice, 2018). The MRO industry also has to account for a large number of personnel performing a large number of tasks and airplanes, maintenance data, and tools that are quickly becoming more digital. The greatest threat faced by the MRO industry, however, appears to be its own unpreparedness. Oliver Wyman's 2018 MRO Survey found that only 50% of OEMs, 41% of airlines, and 9% of MROs have supply chain security standards and fewer than half of all respondents performed a cybersecurity threat assessment in 2017 (Costanza & Prentice, 2018, p. 9).

Known issues. There are two high-level categories of vulnerabilities in aviation maintenance: software and digital data. Software installation and upgrade can occur at many times during an airplane's lifecycle by OEMs, airlines, and MROs. Software tampering at any of these points, for example, may result in interruptions to health and usage data monitoring, which are used to diagnose in-flight issues and prepare for maintenance (Anton, 2017). Software is also used in other aspects of aviation maintenance, such as inventory management, supply chain communication, digital data access, and system diagnostics. *Digital data* includes aircraft communication, addressing, and reporting system (ACARS) data and maintenance data (Anton, 2017), but it is a broad category that also includes ships' records, electronic signatures, proprietary information, audit results, and records containing personally identifiable information. The illicit obtainment of an electronic signature, for example, could be used to forge counterfeit maintenance records.

Purpose

This article is presented to encourage the discussion of cybersecurity in aviation maintenance and the role of SMS in its assurance. At this time, it is appropriate to ask whether current SMS practices and tools can be applied to the mitigation of aviation maintenance cyber threat and cyber risk. It is suspected that some gaps in the SMS framework exist and will need to be addressed if SMS shall be the methodology by which cybersecurity issues are addressed.

Method

S-W-O-T

A SWOT (strengths, weaknesses, opportunities, threats) analysis is a useful tool that helps to identify and categorize aspects of the internal and external environment. In this study, the environment shall consist of the MRO industry, and the SWOT analysis template shown in Figure 1 will be populated with its internal strengths and weaknesses and external opportunities and threats.

STRENGTHS	WEAKNESSES
OPPORTUNITIES	**THREATS**

Figure 1. SWOT analysis template.

SMS

The FAA (2017) recognizes four components of an SMS: safety policy, safety risk management, safety assurance, and safety promotion. An effective SMS consists of all four components, but the level to which each is necessary may depend on the internal and external contexts in which the SMS is operating. A SMS, therefore, is constantly adapting to cultural change within the organization, the organization's business need, public policy, technology advances, and current events.

A review of the four components of SMS indicates that all of them are necessary, because they rely upon each other. Safety policy refers to documented standards, including policies and procedures, training, and controls. These artifacts describe responsibility, accountability, and authority of management's expectations for the organization, and how these expectations will be met; the value of safety in the organization's culture is evident through the safety policy (Stolzer, 2017). When processes and expectations are clearly defined, both through safety policy and the quality management system, the safety risk management process becomes a lot easier to execute. Safety risk management includes hazard identification, risk analysis, and risk control. Stolzer stated that an effective risk management system collaborates both internally (such as within the organization) and externally (such as within the industry) and treats risk management as an ongoing, iterative process. Safety risk management and safety assurance are closely linked; the process of safety risk management allows for safety assurance to be successful because it requires processes and expectations to be defined and risk to be managed to an acceptable level. Safety assurance then goes one step further and measures the success of safety risk management through management review of quantitative observation of output. Safety assurance also includes collecting information from members of the organization via internal and external audits and voluntary reporting. The SMS most successfully collects data in a safety culture. Stolzer described safety promotion as a top-down process beginning with executive leadership and trickling down to individual employees through safety policy. However, safety promotion does not only begin and end within the organization; regulation and collaborative task forces also have power to educate about and encourage best practice of safety management.

Results and Analysis

A review of available literature indicates that very little is known about cybersecurity and its weaknesses in the MRO industry, specifically. Figure 2 organizes the findings into internal strengths and weaknesses and external opportunities and threats categories.

STRENGTHS	WEAKNESSES
Developed cybersecurity assessment and implementation tools, such as International Air Transport Association (IATA) Aviation Cyber Security Toolkit, for other aspects of aviation	Global exchange of MRO services and lack of global cybersecurity standards Large supply chain Lack of extensive background checks for maintenance personnel (Corretjer, 2018) Lack of clearly identified aviation maintenance cyber risks and hazards Low rate of cybersecurity awareness and preparedness among MROs High reliance on digital communications
OPPORTUNITIES	**THREATS**
ICAO involvement Adaptable FAA SMS framework	Increasingly digital inputs (airplanes, data, tools, etc.) Software or digital data tampering may not be evident

Figure 2. SWOT analysis for the MRO industry.

Both internal and external to the MRO industry, there are support organizations with established cybersecurity and SMS processes that can be adapted for use. Some of the internal weaknesses and external threats may be resolved by an MRO-specific standard cyber risk management process, such as the lack of global cybersecurity standards, maintenance personnel background checks, and cybersecurity awareness and preparedness among MROs. Other items in these two categories can be addressed via the safety risk management function of an SMS or cannot be helped at all.

Conclusions and Recommendations

The body of knowledge does not currently contain enough information about cyber risk and hazards in the MRO industry to make reasonable judgments about the SMS framework. This should not, however, deter organizations from considering cyber risks and hazards in their current SMSs. Safety risk management should include cyber risks, such as potential data manipulation and theft and counterfeit data and parts. Risk should be assessed and communicated both within the immediate organization and throughout the supply chain as part of the safety assurance function. Through these two activities, the MRO industry can communicate with its counterparts in the broader aviation community and bodies such as ICAO and the FAA can help establish the safety policy that is seriously lacking today. Safety policy can then address remaining weaknesses by ensuring personnel are trained and trusted and stakeholders throughout the supply chain and around the world are striving to meet the same cybersecurity standards. ICAO and the FAA can also foster safety promotion by challenging individual organizations to continuously evaluate their cybersecurity measures as they would any other SMS policies and procedures.

References

Abeyratne, R. (2011). Cyber terrorism and aviation-national and international responses. *Journal of Transportation Security, (4)*4, 337-349. doi: 10.1007/s12198-011-0074-3

Anton, J. (2017). *Cybersecurity; an EASA perspective on developments and challenges*. Retrieved from https://www.iata.org/whatwedo/workgroups /Documents/ Paperless_Conference_2017/Day1/1100-1130_Cybersecurity_EASA.pdf

Costanza, D. & Prentice, B. (2018). *MRO survey 2018: Tackling industry disruption*. Retrieved from https://www.oliverwyman.com/content/dam/oliver-wyman/v2/ publications/2018/ april/MRO-Survey-2018-web.pdf

Corretjer, P. J. (2018). *A cybersecurity analysis of today's commercial aircrafts and aviation industry systems* (Master's thesis). Retrieved from ProQuest Dissertations and Theses Global. (10745748)

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10), 13-21. Retrieved from http://search.proquest.com.ezproxy.libproxy.db.erau.edu/docview/1638205509?accountid =27203

Federal Aviation Administration. (2017). *Safety management system components*. Retrieved from https://www.faa.gov/about/initiatives/sms/explained/components/

Higgins, J. (2017). DHS' Manfra details efforts to secure aviation sector from cyber attacks. *Inside Cybersecurity*. Retrieved from http://search.proquest.com.ezproxy.libproxy.db.erau.edu/docview/1963863433?accountid =27203

International Civil Aviation Organization. (2016). *Addressing cybersecurity in civil aviation*. Retrieved from https://www.icao.int/Meetings/a39/Documents/WP/wp_017_en.pdf

McAfee. (2018). *Economic impact of cybercrime—no slowing down.* Retrieved from https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf

Stolzer, A.J. (2017). *Safety management systems in aviation*. New York, NY: Taylor and Francis.