ORGANIZING AIR FORCE MAJOR COMMANDS FOR TODAY'S CYBERSECURITY CHALLENGES

GRADUATE RESEARCH PAPER

Jonathan M. French, Major, USAF

AFIT-ENS-MS-17-J-026

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENS-MS-17-J-026

ORGANIZING AIR FORCE MAJOR COMMANDS FOR TODAY'S CYBERSECURITY CHALLENGES

GRADUATE RESEARCH PAPER

Presented to the Faculty

Department of Operational Sciences

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Operations Management

Jonathan M. French, MS

Major, USAF

June 2017

AFIT-ENS-MS-17-J-026

ORGANIZING AIR FORCE MAJOR COMMANDS FOR TODAY'S CYBERSECURITY CHALLENGES

Jonathan M. French, MS
Major, USAF

Committee Membeship:

Major Benjamin T. Hazen, PhD
Chair

Abstract

The scope and scale of cyberspace threats has evolved in parallel to the dramatic increase in global dependence on Information Technology (IT) capabilities in the Information Age. However, cybersecurity capabilities continue to lag the threat in fighting for freedom of maneuver and access in the global commons of the Internet. Industry continues to adapt their cybersecurity programs and organizational design to meet these challenges, yet the Department of Defense and military services have struggled to keep pace with the ever-changing threat environment.

This research pursues a systematic literature review to analyze the evolving landscape of cyberspace threats, industry best practices for managing cybersecurity programs, and current trends in setting up the required supporting organizational structure. The overall objective of the research is to highlight key areas where Air Force Major Commands could improve processes and organizational structures to posture for cybersecurity challenges in the Information Age.

Acknowledgments

I am very thankful for the support that I have received from the ASAM class and the larger cybersecurity community to complete this research paper. I would like to thank Lt Gen Bill Bender, Mr. Pete Kim, Maj Jeremy Sparks, Mr. John Visneski and the venerable Mrs. Pam Bennett-Bardot for their immense support and guidance during this project. Many thanks to Maj Ben Hazen and Col "Data" Bryant, my co-advisors, for both helping scope this project so I could head down the right path and giving me the latitude to explore the space.

Finally, I would like to recognize my wife for leasing my "plentiful free-time at IDE" to pursue this endeavor. I owe you some date nights, rounds of golf, and weekend retreats in the years to come.

Jonathan M. French

Table of Contents

List of Figures

List of Tables

ORGANIZING AIR FORCE MAJOR COMMANDS FOR TODAY'S CYBERSECURITY CHALLENGES

I. Introduction

Background and Motivation

The dawn of the Internet era ushered in an unprecedented wave of cyberspace capabilities that changed the world. E-commerce enabled economic globalization, social media brought local events to the international stage, and automation increased efficiency in almost every sector of industry. It is difficult to find even the smallest part of daily life that is not dependent on some form of information technology.

While cyberspace is ubiquitous in society, so are the multitude of threats that seek to exploit it for gain. Historically speaking, cybersecurity seems to lag the IT sector in producing capabilities needed to secure the advantages of an Information Age world.

The Air Force is not immune to the challenges of cybersecurity, and perhaps is a more lucrative target than many sectors of industry. However, the Air Force's means to approach the cybersecurity problem at the Major Command (MAJCOM) level and above has largely remained stagnant for nearly a decade. With a corporate-wide focus on the increasing cyberspace dependencies and their associated threats, it is imperative that Air Force MAJCOMs understand cyberspace risk to their missions and have a means to include it in their operational decision-making. Organizing the structure of the MAJCOM staff to assume an increased role in cybersecurity is an operational imperative for the Air Force to be successful in the Information Age of warfare.

Research Objectives/Questions/Hypotheses

The purpose of this research is to determine key considerations for the restructuring the Air Force MAJCOM staffs to better posture for cybersecurity challenges in the Information Age. This research answers the following questions through a systematic literature review (SLR):

1. Has the increased cyberspace threat changed the way that industry approaches cybersecurity?

2. What are the roles and responsibilities of cybersecurity entities in the public and private sector?

3. What are the key considerations for creating an organizational structure that is postured for today's cybersecurity challenges?

The hypothesis is that the roles and responsibilities for managing cybersecurity in the Air Force are misaligned with industry best practices. By adopting industry best practices, the Air Force could improve its cybersecurity posture to better assure the core missions in the Information Age.

Research Focus

This research focuses on public and private sector best practices for organizing cybersecurity personnel and capabilities to confront the increasing threat in cyberspace. The research will first look at the current operational environment in cyberspace to assess if there are any major trends that may drive a change to the organizational structure of Air Force Major Commands. The research will then identify core requirements of a cybersecurity program and analyze the roles and responsibilities of the key players.

Finally, the research will identify key considerations for creating an organizational structure postured for cybersecurity.

Assumptions/Limitations

To analyze the problem, the following assumption and limitations are made:

Assumption 1: The cybersecurity threat environment in the private sector is similar in magnitude to that in the public sector.

Limitation 1: Due to limited traditional academic research on the topic of organizing cybersecurity personnel, industry-produced research will be required to help form the basis of the literature used in the SLR.

Limitation 2: Budgetary constraints for the ASAM program will limit the number of sources that can be purchased for this study.

Limitation 3: Classified information on cyberspace threats or cybersecurity tactics, techniques, and procedures (TTPs) will not be included in this research.

Implications

The purpose of this research is to determine key considerations for restructuring the Air Force MAJCOM staffs to better posture for cybersecurity challenges in the Information Age. The current organizational structure as well as the roles and responsibilities for cybersecurity entities are hotly debated within the Air Force, with little mutual understanding of the options available to leadership that leverage lessons learned in industry.

This research will identify and recommend best practices for organizing cybersecurity personnel to help MAJCOM staffs understand the costs and benefits of one

method over another. Ultimately, the ideal organizational structure depends on the unique requirements of the MAJCOM Commander.

II. Methodology

Chapter Overview

This chapter discusses how the systematic literature review serves as a means to evaluate the current cyberspace threat environment and how organizations are structuring cybersecurity programs to confront the threat.

Identification of Sources

A systematic literature begins with identifying an exhaustive list of pertinent literature based upon certain inclusion criteria while also creating exclusion criteria to minimize the amount of irrelevant material gathered (Durach, Wieland, & Machuca, 2015). In the cybersecurity realm, identifying proper inclusion and exclusion criteria served to be a particularly challenging concept as much of the "thought leadership" on the topic is found in industry as opposed to traditional scholarly articles. Additionally, with the rapidly changing operational environment, articles that are greater than five years old tend to be stale in content or concepts, leading to a much narrower body of work serving as the relevant material for examination (Westby, 2015).

Google Scholar, EBSCO host, and the United States Air Force Expeditionary Center librarian were used to identify potential sources. A broad search was conducted to identify the breadth and depth of scholarly material that was present in the research space. Searches for terms such as "CISO" or "cybersecurity" returned results in the tens or hundreds of thousands. Changing the search query to targeted keywords such as "CISO role" returned a more manageable result. Narrowing the date range to within the last 5 years further refined the returns.

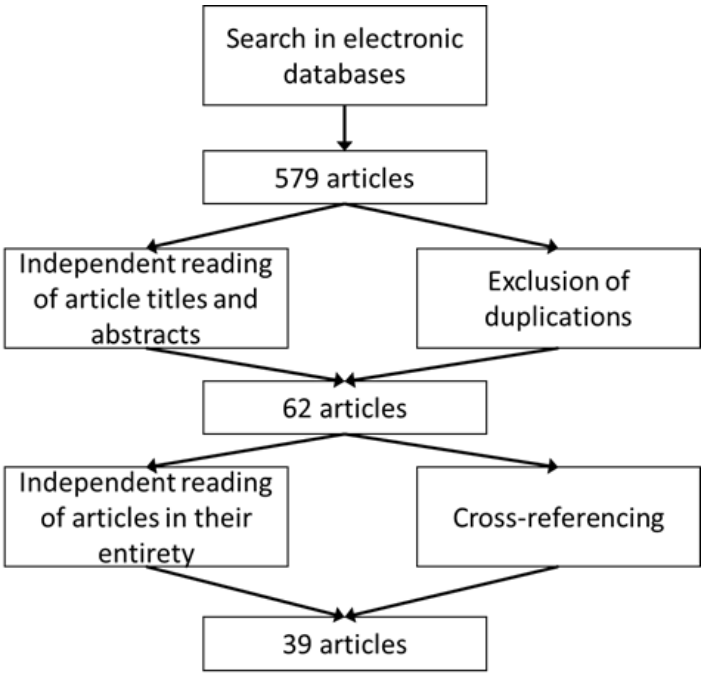


Figure 1. Source selection process

After the initial search in electronic databases, returns were screened using inclusion and exclusion criteria. The initial round of screening involved reading 579 article titles to see if the subject material was relevant to the research questions. Articles were excluded by title for several reasons. The first reason for exclusion was that the article was focused on a technical aspect of CISO duties, such as specific ways to implement a critical infrastructure framework from the CISO office or best practices to secure a cloud hosted application. The majority of the results were eliminated due to meeting this exclusion criteria. The next reason why articles were excluded is because the term "CISO" has alternate meanings outside of cybersecurity and were irrelevant to the study. Finally, articles that were obviously very narrow in scope were eliminated as this study is a strategic look at the organizational construct for cybersecurity rather than

focused on best practices for specific responsibilities within the cybersecurity entity itself.

After excluding articles by reading only the titles, the researcher eliminated duplicative results and proceeded to review the abstract of each remaining article to determine relevance to the research questions. Articles were immediately eliminated if an abstract or conclusion was not available for review. Also, articles were eliminated if the abstract was overly vague and did not clearly relate to the stated title or the research questions. Again, articles were eliminated if the abstract showed that they were technical in nature, such as proposing a technical, enterprise architecture-based method to implement the CISO roles in an organization.

Of the 579 articles returned during the initial query, only 62 articles were included after the round of title and abstract filtering. Of those articles, 33 met the previously stated inclusion and exclusion criteria and were and were available in the full text. Four additional articles that met the criteria were purchased for use as their abstracts aligned perfectly with the research questions. One of those four articles was ultimately eliminated because the purchase only produced an abstract, and the authors were unable to produce the article for the researcher.

Further cross-referencing of the remaining literature expanded the list of included articles by three additional articles, for a total of 39 included articles. For example, a report from the U.S. House of Representatives fit this model (Upton, 2015), as it was referenced in an article found during discovery but was not identified in the results returned from the discovery itself. This article was included because it identified findings by Congress on the shortcoming of the cybersecurity organizational construct of another

Federal entity, the Department of Health and Human Services. Figure 1 represents the process for the systematic literature review.

Expansion of Research to Include Defense-Related Issues

From the sources identified in the systematic literature review process, only three directly pertained to defense-related cybersecurity issues. Therefore, additional research was necessary to find defense-related literature that aligned with the common themes found in the academic and industry material. This material was located through a more generalized Internet search engine query, targeted searching of Internet interest groups on social media, and requesting Air Force specific literature from the Headquarters Air Force and various other cybersecurity entities in the service.

Although the study focused on the evolving context of the cyberspace environment and how that can drive changes to the way that cybersecurity is organized, the applicability to military operations is relatively unique. Identifying the specific threats to military operations in cyberspace, and the tailored actions that are being taken to address those threats is imperative to understanding if the private sector organizational structures apply to the Air Force and its MAJCOMs.

Categorizing Findings from the Available Literature

Data from the systematic literature review were extracted and categorized according to the research questions identified in Chapter I. The categorization only analyzed those items that were core themes among the preponderance of literature. This was necessary to mitigate the potential for bias of the researcher and prevent steering the outcome of the study to specific pre-determined conclusions.

Table 1. Data Categorization of Sources

Category	Relevant Articles
Background (Military)	(Bender, 2016; Bender & Bryant, 2016; Brasington & Park, 2016; Evans, 2009; Libicki, 2012; Mollison, 2015; Pritchett, 2012; Rosello et al., 2014)
Cyberspace Threats (Military)	(Brasington & Park, 2016; Bryant, 2015, 2016; S. J. Fox, 2016; Frodl, 2012; Lohrmann, 2014; Moteff, Copeland, & Fischer, 2003; Roesener, Bottolfson, & Fernandez, 2014; Trump, 2017; Wilson et al., 2016)
Cyberspace Threats	(BAE Systems, 2017; Focal Point Data Risk, 2017; D. Fox, 2013; Goldman, 2017; Knapp & Boulton, 2006; Kotabe, 2005; Mollison, 2015; Rosello et al., 2014; Wagner & Disparte, 2016; World Economic Forum, 2017)
Role of Boards and Executives	(BAE Systems, 2017; Bell, 2017; Bohmayr, 2017; Focal Point Data Risk, 2017; Hamblen, 2017; National Association of Corporate Directors, 2017; Sweeney, 2016; Veltsos, 2017; Westby, 2015; Williams, 2016d)
Role of CIOs	(Bender, 2016; Boulton, 2016; McKinty, 2017; National Association of Corporate Directors, 2017; Sheridan, 2016; Williams, 2016d)
Role of CISOs	(BAE Systems, 2017; Boulton, 2016; Christiansen, 2015, 2016; Cobb, 2015; Focal Point Data Risk, 2017; Geer & McClure, 2016; Grossman, 2017; Institute for Applied Network Security, 2017b; Jones, 2016; Rashid, 2015; Sheridan, 2016; Sweeney, 2016; Upton, 2015; Westby, 2015; World Economic Forum, 2017)
Cybersecurity Organizational Structures	(Boulton, 2016; Christiansen, 2016; Focal Point Data Risk, 2017; Grossman, 2017; Institute for Applied Network Security, 2017a, 2017b; Jones, 2016; Rashid, 2015; Sheridan, 2016, 2017; Upton, 2015; Veltsos, 2016, 2017; Westby, 2015; Williams, 2016a; Winnefeld, Kirchhoff, & Upton, 2015)

Summary

This chapter discussed how the systematic literature review serves as a means to evaluate the current cyberspace threat environment and how organizations are structuring cybersecurity programs to confront the threat.

III. Analysis and Results

Chapter Overview

There is a dearth of research specifically aimed toward finding better ways to organize cybersecurity personnel and capabilities. As such, a systematic literature review was conducted in order to uncover relevant themes pertinent to the research questions.

By the end of this literature review, the reader should have sufficient understanding of the current environment in cyberspace and its associated threats. Furthermore, the reader should know the general areas that are key to a strong cybersecurity program. Finally, the reader should understand the roles and responsibilities of key entities that manage cybersecurity within an organization, and various considerations for organizing cybersecurity capabilities.

RQ1: Has the Increased Cyberspace Threat Changed the Way that industry Approaches Cybersecurity?

Dependence on Cyberspace Capabilities

Cyberspace is defined in joint doctrine as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (U.S. Joint Chiefs of Staff, 2013). As information technology (IT) and cyberspace have become ubiquitous over the last decade, an increasing number of vital national power centers depend on its availability. Cyberspace includes more than just computers and networks, with cyberspace capabilities underpinning various societal

staples to include aircraft avionics, the banking industry, industrial controllers and even most modern cars (Bender & Bryant, 2016).

The United States military is not immune to the global dependence on cyberspace. Since the dawn of the Internet era, the military has been a rapid adopter of networked systems to facilitate the execution of both lethal and non-lethal operations (Libicki, 2012). As such, virtually every military operation from the tactical through the strategic level relies on the availability, quality and quantity of information communicated through the domain (Pritchett, 2012). Therefore, it stands to reason that an attack on the Department of Defense's information systems has the potential to disrupt the Nation's ability to rapidly project precision combat power against its adversaries abroad (Mollison, 2015).

As the U.S. military's "high tech" service, the Air Force is perhaps the most dependent on cyberspace capabilities. Since 9/11, many new technologies have been ushered in as a means to enhance global vigilance to confront the threat of terror (Bender, 2016). The proliferation of infrastructure, sensors, and systems aboard weapons platforms proceeds without any end in sight, creating a complex web of capabilities that actually complicates the service's ability to compete against a near-peer adversary in an anti-access/area denial (A2/AD) environment (Bender, 2016).

The implicit assumption of the Air Force's IT-based capability development was that its systems would operate in a fundamentally permissive environment, with signals intelligence being the greatest adversarial threat (Bryant, 2016). However, inadvertent interruptions caused by failing air conditioning units in data centers, misguided construction digs, or an anchor dragging across an undersea cable have had

a massive negative impact on the availability of the service's cyberspace-based systems (Bender & Bryant, 2016). Further increasing the complexity of the problem, many critical mission dependencies reside outside of the purview or control of Air Force personnel, such as power generation, power distribution, and commercial network backbones (Bryant, 2015). Therefore, the Air Force is seeking to maintain an enterprise architecture that can easily onboard new technology without a burdensome integration effort (Bender, 2016). This architecture will help the Air Force enter the Information Age of warfare with a sense of urgency (Bender, 2016).

The efficiency and scale of the world's modern logistics system is unimaginable without the connectivity of the Information Age (Brasington & Park, 2016). Critical enabling functions such as controlling passenger transportation, inventory tracking, vehicle operations, and pipeline operations rely heavily on cyberspace capabilities and often lack the required security controls (Evans, 2009).

The global nature of Air Mobility Command's (AMC) mission demands the use of computers, IT systems, and network infrastructure in both its day-to-day and wartime mission (Rosello et al., 2014). Also, close partnerships with the Civil Reserve Aircraft Fleet (CRAF) drive requirements to share digital information through unclassified mediums with private sector corporations (Rosello et al., 2014). For example, AMC's aerial ports and deployed forces use an in-transit visibility (ITV) system called GATES to process, manifest, and track passengers and cargo. Joining LOGMOD, DCAPES, CMOS and ICODES as part of a family of systems known as the Integrated Deployment System (IDS), GATES presents a significant cyberspace

dependency for Air Mobility Command that could impact Combatant Commander visibility on logistics and supply chain management if degraded (Mollison, 2015).

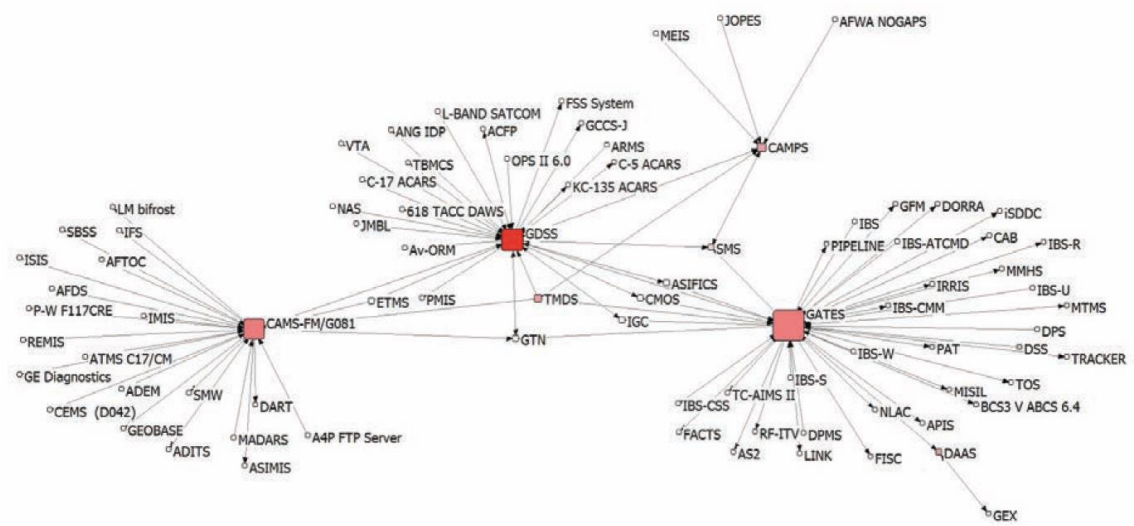


Figure 2. Information Exchanges between Logistics IT systems (Rosello et al., 2014)

Understanding the Cyberspace Threat

The natural synergy between organized crime and the Internet has decreased the security of the digital world (Kotabe, 2005). With both large and small corporations as the most common target of such groups, business leaders typically feel that no matter how much money they throw at cybersecurity, they will still get breached (Focal Point Data Risk, 2017). Although most aggressors against corporate interests are common criminals, some more advanced threats have surfaced recently. However, foreign governments are still far more likely to breach a network for intelligence on military capabilities or trade secrets while organized crime seeks to create financial gain (Mollison, 2015).

In October 2016, attackers executed a distributed denial of service (DDoS) attack on a Domain Name Service (DNS) company called Dyn that shook the

cybersecurity industry (World Economic Forum, 2017). While the vulnerability that led to the attack was not directly the responsibility of Dyn, poor cybersecurity practices from its external partners are most likely to blame for the attack (World Economic Forum, 2017). Such complex dependencies on the cyberspace domain both internal and external to an organization paint a dire picture for public and private leaders. According to a report from the Identity Theft Resource Center (ITRC), there was a 40% increase in the number of reported data breaches in 2016, representing an all-time high of 1,093 against 780 in the previous year (Goldman, 2017). Drilling into the statistics, the business sector had the most breaches with 494, while the financial sector had the least with only 52 reported incidents (Goldman, 2017).

Even with the number of reported events increasing each year, there is still a significant lack of awareness of the threat. In late 2016, more than 200 C-suite representatives from Fortune 500 companies were interviewed to examine trends in threat awareness. More than 68% of IT decision makers and 75% of C-suite respondents noted that they expect the number of attacks to increase in the next year (BAE Systems, 2017). Also, about 67% of respondents believe the severity of attacks will increase in that same time frame (BAE Systems, 2017). Although IT and C-suite personnel have a general feel for the threat, most users do not attribute the cause of a system malfunction or error to a possible breach (Rosello et al., 2014). This disparity of awareness between the average employee and the corporate leadership could mean that many breaches are unreported or go unmitigated for longer than necessary.

The U.S. military faces significant challenges in the cyberspace domain. Due to the military's role in national defense, its adversaries in cyberspace have a clear

interest in creating havoc during combat operations, while needs are the highest (Libicki, 2012). Making the situation even direr is that America's adversaries clearly understand the military's vulnerability to attack, and often train and organize to exploit it (Bryant, 2015).

In his 11 May 2017 Executive Order, President Trump noted that "unmitigated vulnerabilities are among the highest cybersecurity risks" and are often the result of maintaining end-of-lifecycle systems or failure to execute specific security configuration guidance (Trump, 2017). The military struggles to balance the requirement to refresh outdated systems with shrinking defense budgets that must also account for major weapons acquisitions. While the military juggles these demands, threats to existing systems proceed at a pace and sophistication never seen before (Wilson et al., 2016).

Cyberspace threats extend well beyond the traditional computer networks and into operational technology such as industrial control systems, weapons platforms, and mission partners (Bryant, 2016). For example, threats to Defense Industrial Base networks represent what then Deputy Secretary of Defense Ashton Carter called "unacceptable risks [that] pose an imminent threat to US national security and economic interest" (Roesener et al., 2014).

President Bill Clinton signed Executive Order 13010 on 15 July 1996, which established the President's Commission on Critical Infrastructure Protection. In the order, critical infrastructure is defined as "certain national infrastructures so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States" (Moteff et al., 2003).

Specific transportation capabilities were identified as critical infrastructure, to include national airspace systems, airlines, aircraft, airports, ports, maritime vessels, freight and passenger rail, and delivery services. The nation's dependence on critical infrastructure extends well beyond the military and economic realm. Unseen to date, many cybersecurity experts ponder the impacts of a deliberate attack on U.S. critical infrastructure that could require weeks or even months to restore (Lohrmann, 2014).

Over the past six years, cyberspace threats to aviation and other transportation means have increased in both quantity and sophistication. Although only a small part of the overall critical infrastructure challenge, transportation extends well beyond national borders and presents a particularly complex problem to solve for cybersecurity professionals. As a whole, the industry is so highly reliant on timeliness and reliability that even the smallest delay due to an intrusion could have massive and even global implications (Brasington & Park, 2016).

In 2015, the European Aviation Safety Agency (EASA) hired an expert to test the cybersecurity of the Aircraft Communications Addressing and Reporting System (ACARS). The expert penetrated the system within 5 minutes and gained access to aircraft control systems over just a few days (S. J. Fox, 2016). Around the same time, a Polish airline grounded several aircraft after a ground operations system was compromised, preventing the development of flight plans (S. J. Fox, 2016).

In the shipping business, low-end cyber-attacks have successfully disrupted what appears to be an industrial-aged industry. However, the truth is that shipping is heavily dependent on information technology and leverages many trust-based relationships between mission partners to promote in-transit visibility (Brasington &

Park, 2016). In 2011, hackers breached the Antwerp port's IT network and used stolen data to intercept illicit goods before the port authority could inspect them (Brasington & Park, 2016). Additionally, there are numerous reports of Somali pirates hacking into shipping operations centers to take over the unprotected data channels of ships at sea, facilitating a limited-duration pillage of only high-value goods (Frodl, 2012).

The Need for a Strong Cybersecurity Program

Many companies have strong beliefs that they are not the target of malicious actors in cyberspace. The fact that they have not been a victim of an attack reinforces that belief and acts as a disincentive to investing in cybersecurity expertise, technology or assessments (D. Fox, 2013). However, companies that have fallen victim to a cyber-attack often say that there are only two kinds of organizations – those that have been hacked and know it, and those that have been hacked and don't (Freedman, 2015). Once thought of as only a military issue, cyber warfare is now a societal issue and cybersecurity needs to be woven into key systems and process from end to end to build and maintain a competitive advantage (Groysberg & Cheng, 2016; National Association of Corporate Directors, 2017).

Estimating the overall cost of cyber-attacks is difficult, but estimates range between $400-500 billion annually, with many costs deemed to be unreported (National Association of Corporate Directors, 2017). Cybercrime grew by more than 400% between 2013 and 2015, with projections around $2 trillion each year expected by 2019 (Hamblen, 2017). Interestingly, IT personnel estimate the cost of a single cyber-attack to be twice as costly as corporate executives (Hamblen, 2017).

Although cybersecurity is quickly becoming a trendy portfolio item in businesses of all sizes, its role is changing in organizations with a more mature cybersecurity program (Christiansen, 2015). For many, trust is the main value that security brings to the business (Focal Point Data Risk, 2017). While trust is critical both internal to the business and between the business and its customers, it is notoriously difficult to measure.

For most firms, cybersecurity is now a risk issue like any other business risk (BAE Systems, 2017). The perception of cybersecurity risk can vary among different groups within a company, between various stakeholders in a project, and between a board and its shareholders. If a company's data is not compromised, it is hard to prove that resource investments were justified (Williams, 2015). The only near-certainty with cybersecurity is that more resources will be redirected toward the problem after a compromise has occurred.

In a recent survey, 71% of corporate executives named cybersecurity as their most significant business challenge (BAE Systems, 2017). Furthermore, 72% of IT decision makers expect to be targeted by a cyber-attack within the next 12 months (BAE Systems, 2017). Securely operating technology that is inherently unsecure is a massive task that requires more than simply investing in talent and materials (Winnefeld et al., 2015).

Proposition 1: The world is becoming increasingly dependent on cyberspace, a domain which is extremely complex, subject to attacks from capable and determined adversaries, difficult to defend, and can cause significant operational and financial losses, if breached.

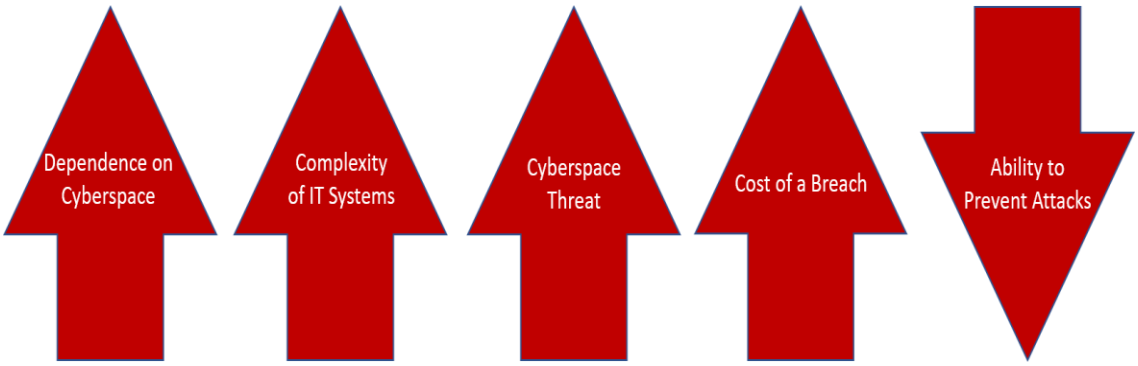


Figure 3. Overview of the Current Cyberspace Environment

Cybersecurity in the Federal Government

During the 2016 U.S. presidential election season, cybersecurity was one of the top three issues to business leaders (Groysberg & Cheng, 2016). In both business and the military, there is wide recognition that most core business operations have not changed. Rather, what is new is the necessity to protect and assure the business through cyberspace (Bender & Bryant, 2016). From the shipping industry to the financial sector, there is a new emphasis on safety and security in the digital world, starting with a firm understanding of cyberspace dependencies and vulnerabilities (Brasington & Park, 2016).

The Global Information Security Workforce Study (GISWS) of 2015 stated "When we consider the amount of effort dedicated over the past two years to further the security readiness of federal systems and the nation's overall security posture, our hope was to see an obvious step forward. The data shows that, in fact, we have taken a step back" (Geer & McClure, 2016). Therefore, many cybersecurity professionals were unsurprised to see the Trump administration announce a new executive order on

11 May 2017 that aimed to tackle the federal cybersecurity readiness problem (Trump, 2017). As an outcome of the order, agency heads are accountable for implementing cyberspace risk management measures that align with strategic, operational, and budgetary planning processes (Trump, 2017). Within 90 days of the announcement, each agency head must document risk mitigation and acceptance choices that have been made along with the considerations that informed the decisions. Any accepted risk from unmitigated vulnerabilities must be identified along with a plan of action to implement the National Institute of Standards and Technology (NIST) Framework (Trump, 2017).

Cybersecurity Imperative: Managing Cybersecurity Risk

Information is the lifeblood of many organizations, yet many organizations struggle to measure the risks associated with how that information is received, stored, manipulated and disseminated throughout the enterprise (Focal Point Data Risk, 2017). The compromise of sensitive information is no longer purely a technical issue, but one of risk and liability for senior leadership (Upton, 2015). As CyberScout CEO Matt Cullina stated, "In an age of an unprecedented threat, business leaders need to mitigate risk by developing C-suite strategies and plans for data breach prevention, protection and resolution" (Goldman, 2017). Getting to a point where cybersecurity is a team sport has proven to be a difficult task for even the most well-established organizations.

From an enterprise perspective, cybersecurity risk has to be "baked in" to organizational processes rather than "bolted on" as an afterthought (Williams, 2016b). Cybersecurity is a serious enterprise-level risk that affects all levels of an

organization's operating activities to include supply chain management, customer relations, and production control. The complexity, speed, and potential for damage from an attack paired with the impossibility of total threat avoidance make cyberspace risks especially troubling (National Association of Corporate Directors, 2017).

Proposition 2: Cybersecurity is no longer a technical issue, but one of managing risk.

Even with the private sector assumption that data is the lifeblood of the company that must be carefully managed by balancing risk, the military culture continues to pursue perfect information (Bender & Bryant, 2016). The military is one of many organizations that has spent vast sums of money to secure its information systems but still maintains a reactive, tactical posture when dealing with intrusions rather than taking a holistic view of cybersecurity as an enterprise-level issue (D. Fox, 2013).

Additionally, the military struggles to change from a mindset of preventing every attack to fighting through attacks while accomplishing the mission (Bender & Bryant, 2016). This notion is an imperative, as the military's dependencies on cyberspace capabilities prevent it from disconnecting from the Internet as a means to thwart adversarial attacks (Williams, 2016c).

Cybersecurity Imperative: Translating Technical Jargon to Business Objectives

One major challenge for cybersecurity personnel is presenting highly technical information in business terms. In recent research, it was found that there was little

consensus on the value of cybersecurity, with board members citing items as most critical that rated last among security professionals (Focal Point Data Risk, 2017). One corporate board member noted that "nobody cares how many packets the firewall blocked. If security does not reflect business goals, you are doing it wrong" (Focal Point Data Risk, 2017). Cybersecurity is not intuitive to many, and weaving security into the fabric of the business is imperative to protecting critical assets (Institute for Applied Network Security, 2017a). With information and data often comprising the majority of a company's value, every interaction with organizational decision makers needs to be treated as an opportunity to teach and must be done in the language of the business (Focal Point Data Risk, 2017; Institute for Applied Network Security, 2017a).

Proposition 3: Cybersecurity issues should be discussed in the core language of the business.

Cybersecurity Imperative: Understanding the Terrain and Assuring the Mission

Recognizing cyberspace as a warfighting domain has led many begin to map cyberspace characteristics in a similar fashion as the physical domains. Key cyber terrain is defined as "those physical systems and logical elements that enable mission essential warfighting functions" (Bodeau, Graubart, & Heinbockel, 2013). Some cybersecurity experts map the technical environment and choose to explain the relationships through analogy with the land domain or by identifying touch points between physical objects and their cyberspace compliment (Bodeau et al., 2013). On the other hand, the Air Force is seeking to ensure that missions and cyberspace mission

dependencies are clearly defined and prioritized which will help identify the key terrain in the enterprise.

Air Force doctrine defines cyberspace mission assurance as "measures required to accomplish essential objectives of missions in a contested environment. Mission assurance entails prioritizing mission essential functions, mapping mission dependence on cyberspace, identifying vulnerabilities, and mitigating risks of known vulnerabilities" (Department of the Air Force, 2011). Military cyberspace leaders are beginning to recognize that the objective should not be to secure the network for its own sake, but must instead stay focused on the mission and assuring dependencies on cyberspace capabilities (Kennedy, 2016). Pursuit of mission assurance in and through cyberspace is much more than an IT problem. Rather, it requires an intricate understanding of the core mission of the organization, the processes involved in planning and executing the mission, and the networks, technology, systems and platforms that enable it (Schulz, Kotson, & Zipkin, 2015). One major component of mission assurance is the ability to conduct operations in an environment in which the enemy has penetrated their networks (Kennedy, 2016).

Cyberspace mission assurance extends beyond the realm of traditional IT and requires a firm grasp of the cyberspace implications of physical systems. Industrial control systems and weapons systems have obvious dependencies in the cyberspace domain and require careful consideration when constructing cybersecurity strategy and policy as the impact of their degradation or compromise is greater than many other IT systems (Bryant, 2016).

Therefore, it is more than just the cybersecurity personnel who need to adapt to the demands of mission assurance. Operations and support personnel must build proficiency in operating in an environment where nothing works as expected (Bender & Bryant, 2016). One of the primary aims for standing up the Air Force's Task Force Cyber Secure was to take an enterprise-level approach to assuring the five core missions in the Information Age of warfare (Bender, 2016). The task force looked across traditional functional lines to advance cyberspace education and culture in the Air Force.

A major outcome of Task Force Cyber Secure was garnering strategic support for creating wing-level cyberspace operations squadrons. These future cyberspace squadrons have a mission of providing wing-level expertise to integrate full-spectrum cyberspace capabilities in, thru and from the domain to accomplish the wing's mission from generation through execution (Kennedy, 2016). For the first time, wing commanders will have the ability to assess their units' readiness in the cyberspace domain and can employ organic capabilities or request support from higher echelons to address events or known deficiencies (Pritchett, 2012). Not only will commanders be able to prioritize missions that require more active cyberspace support, but they can assess causes of interruptions, capture key lessons, and drive improvements to increase mission effectiveness and efficiencies (Wilson et al., 2016).

With a focus on mission assurance, MAJCOMs would be best served to focus on processes, systems, and information that have the highest potential for major mission impact (Rosello et al., 2014). Using the vignette concerning GATES and the rest of the IDS family as an example, aerial ports must be able to continue functioning

during a service interruption, to include capturing mission-essential data from all relevant mission partners (Mollison, 2015). However, as of 2015, unit SOP's failed to address the steps necessary to assure the aerial port mission during a cyber-attack that would cause service interruption or significant degradation (Mollison, 2015).

Proposition 4: Rather than focusing on securing cyberspace capabilities, organizations should emphasize assuring mission dependencies on cyberspace capabilities.

Cybersecurity Imperative: Creating a Culture of Resilience

Many leaders in the cybersecurity industry acknowledge that at some point, every organization will be breached (McKinty, 2017). Therefore, a focus on resilience rather than prevention is becoming a trend in the industry. The Department of Homeland Security's Risk Steering Committee defines resiliency as the "ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption" (Bohmayr, 2017; Bryant, 2015).

Cyberspace resilience is a leadership issue and one that requires strategic oversight at the highest level of the organization (World Economic Forum, 2017). Cyberspace resilience and risk management are closely related, and both must integrate into the overall enterprise-wide risk management, budgeting, and resource allocation strategies to achieve any measure of lasting success (World Economic Forum, 2017).

One method for increasing cyberspace resilience is to introduce rigorous security standards in the procurement and network design processes (Libicki, 2012).

Resilience at the system level is one method to help ensure that disaster recovery (DR) or continuity of operations plans (COOP) support unplanned or emergency scenarios affecting the core business unit (Lohrmann, 2014). Others advocate for focusing on the mission as the objective for resilience, where certain solutions lie completely outside of the cyberspace domain and involve variations in tactics, techniques, and procedures to reduce the dependence on a specific cyberspace capability (Bryant, 2015, 2016).

Proposition 5: Leadership should set the conditions for resilience by ensuring the ability to operate through, and rapidly recover from, disruptions to cyberspace dependencies.

Cybersecurity Imperative: Strengthening Cybersecurity Governance

Cybersecurity is a multi-disciplinary challenge that requires a strong governance framework underwritten by strong leadership, senior executive engagement, and clear accountability (Freedman, 2015). Each business unit should be empowered and accountable for actions or inaction within their respective areas, measured and reported through an enterprise-level governance council. In the private sector, cybersecurity councils are chaired by either the CEO or CISO and have diverse executive-level representation from the C-suite (COO, CFO, CIO, CSO) and the business units (Allen et al., 2015). The council's objectives can include reviewing the status of cybersecurity objectives and requirements, implementation of cybersecurity plans, programs and policies, and assessing compliance with externally imposed security obligations (Allen et al., 2015; Lohrmann, 2014)

Proposition 6: A strong cross-functional cybersecurity governance program should be underwritten by senior leadership as governance provides the framework for the organization's success in cyberspace.

RQ2: What are the Roles and Responsibilities of Cybersecurity Entities in the Public and Private Sector?

Role of the Boards and Executive Leadership Team

In the private sector, the ultimate responsibility for cybersecurity and cyberspace resilience rests with the board and senior executives (Bohmayr, 2017). This responsibility is important, as corporate leadership must push cybersecurity culture change throughout the layers of the organization (Institute for Applied Network Security, 2017a).

However, in a survey of 221 CEOs and 984 IT decision makers, each respective group pointed to the other for ultimate accountability in the event of a breach (Hamblen, 2017). With virtually no exceptions in the literature review, all researchers proposed that the risk owner should be the executive who covers the losses if the risk materializes (Jones, 2016). Specifically, the CEO or agency head is identified as singularly responsible for accepting risk.

President Trump echoes this sentiment in his recent executive order on cybersecurity. In the text, he directs departments and agencies to "document the risk mitigation and acceptance choices made by each agency head as of the date of this order" (Trump, 2017). This directive does not strip the CIO or CISO, as the IT decision makers, of any responsibility or accountability. It is still imperative that they

build alliances for a risk-based approach that facilitates the business owning the risk, with business leaders accountable for risk acceptance (Sheridan, 2017).

Proposition 7: The senior executive of the organization is the ultimate owner of cybersecurity risk as he or she is accountable if the risk materializes.

As the threats in cyberspace have become more widely known, different levels of public and private organizations have been trying to figure out their role in cybersecurity. Tom Ridge, former Secretary of the Department of Homeland Security noted that "cybersecurity is the most significant governance challenge for the public and private sector. It is not just the exclusive domain of the CIO and CTO. It is now in the domain of the CEO and the corporate board" (Hamblen, 2017). That message was echoed by the board of Yahoo when they voted to take away the cash bonus of CEO Marissa Mayer for failing to properly comprehend or investigate the severity of cyber-attacks responsible for breaching 500 million user accounts (Bell, 2017). As a follow on measure, the board directed senior executives to fortify the company's cybersecurity and incident response measures to ensure "escalation of cybersecurity incidents to executives and the board" (Bell, 2017).

As technology-based value creation has dramatically increased over the past decade, senior executives and boards have given greater attention to cybersecurity and resilience (Bohmayr, 2017). Many companies have even begun to look towards cybersecurity and resilience as a source of competitive advantage (Bohmayr, 2017). In that regard, boards and C-suite executives have taken responsibility for mitigating business and cybersecurity risk, while the IT department retains ownership of

delivering the technological support that drives the business (McKinty, 2017). It is important that corporate leadership treat cybersecurity as a strategic, cross-departmental, enterprise risk management issue rather than a stand-alone indicator of IT readiness (National Association of Corporate Directors, 2017).

In the leadership role, boards should clearly establish what the business needs from the cybersecurity program and not assume that it is known by subordinate management (Focal Point Data Risk, 2017). In a poll of Fortune 500 companies, 96% of corporate boards assess strategic risk, 89% discuss cybersecurity, and only 41% include cybersecurity in the overall discussion of risk (National Association of Corporate Directors, 2017).

Corporate leadership must know their cybersecurity posture as well as their response actions for an attack, but more than 40% of corporate boards admit to not having a clear understanding of cybersecurity protocols (Sweeney, 2016). Understanding such measures is quickly becoming part of the job description for senior leaders, and requires an enduring relationship with cybersecurity personnel in place of annual reviews or periodic updates (Sweeney, 2016). Together with cybersecurity personnel, boards must discuss lessons learned from previous incidents, understand fix actions, and ensure that incident response actions are updated (Veltsos, 2016). Overall, an in-depth understanding of the cybersecurity strategy is critical if executives are to effectively assess or combat risks and be accountable for the fallout from future breaches (BAE Systems, 2017).

In a sign of changing times, some corporate boards have taken an active role in changing the organization to maximize effectiveness in handling cybersecurity risk

(Westby, 2015). In a dramatic increase from 2008 when only 8% of boards stated they created a risk committee separate from the audit committee, 53% of corporations had a separate committee in 2015 (Westby, 2015). Additionally, boards are working to ensure that privacy and security roles in the organization are separated and appropriately aligned (Veltsos, 2016).

Proposition 8: Boards and executive leadership should take an active role in maximizing the effectiveness of the cybersecurity program.

Role of the Chief Information Officer (CIO)

The role of the Chief Information Officer (CIO) differs from organization to organization and varies widely between the public and private sector. In many organizations, the CIO is the primary executive responsible for the leadership and vision for IT implementation that propels the business forward (Sheridan, 2016). In organizations that require innovation to survive, strong CIOs are typically the ones leading the charge (Boulton, 2016; Sheridan, 2016).

However, in many organizations, the CIO is frequently relegated to technical issues such as outsourcing IT support, moving systems to the cloud, and ensuring network availability (Sheridan, 2016). In the Air Force and the federal government writ large, CIOs are commonly responsible for the development, implementation, management, and operation of IT across the department (Upton, 2015). The tactical compliment of the Air Force CIO is the base communications squadron. With the shift to mission assurance, the Air Force is partitioning the IT support roles of the squadron

into a largely outsourced communications element with a mission to plan, install, operate and maintain IT systems and support services (Kennedy, 2016).

A common complaint in many companies is that the CIO needs to be better equipped to articulate the interaction between IT and cybersecurity from both a risk and ROI perspective (Williams, 2016a). In many organizations, CIOs are juggling so many of the business's top priorities that overall perceptions of their performance are dropping. In a recent survey, 50% of corporate executives polled believe that human error in the IT department would be the contributing factor for a successful cyber-attack (McKinty, 2017). In another survey, more than 60% of IT staff said that they do not report cybersecurity concerns until they are urgent, and acknowledged trying to minimize negative results (National Association of Corporate Directors, 2017).

Proposition 9: CIOs should assume the role of a visionary and primary driver of innovation through the implementation of IT solutions that propel the core business forward.

Role of the Chief Information Security Officer (CISO)

Over the last few decades, a new executive role has emerged to focus solely on cybersecurity. This new entity, known as the Chief Information Security Officer (CISO), originally sat in the IT department, managing firewalls and other mainstays of the security apparatus (Grossman, 2017). The first CISOs reported to the CIO who filled the role of the lead technical expert within the organization (Grossman, 2017).

In 2008, only 30% of Forbes Global 2000 companies in the private sector reported having a CISO in their ranks (Westby, 2015). Moving into the era of frequent cyber-attacks, that number rose to 73% in 2015 and continues to climb (Westby,

2015). The increase in prominence of the CISO in light of increasing cybersecurity threats was one of the biggest business trends in 2015 (Cobb, 2015). Still, many large companies either lack a CISO or are in the process of hiring one, typically after suffering a major breach (Geer & McClure, 2016).

In a survey conducted by Focal Point Data Risk, one board member stated, "CIOs and CISOs often talk about what they want their jobs to be. The Board talks about what their main job should be: to protect the business and its liability" (Focal Point Data Risk, 2017). While communication between the CISO and the board is not always great, it is not solely due to differing priorities between the board and the security team (BAE Systems, 2017). The board must ensure that one executive is responsible for managing the cybersecurity and resilience program. That person must have regular access to the board, the appropriate authorities, a firm grasp of the subject matter, and adequate resources to fulfill those duties (World Economic Forum, 2017). In more and more organizations, that executive is the CISO.

The CISO has historically been viewed as purely a technical expert, rising through the ranks of the IT department, under the purview of the CIO (Christiansen, 2015). The main function of the CISO had been to implement security technologies, with an emphasis on infrastructure and internal systems (Christiansen, 2015).

As the cybersecurity ecosystem has transformed, the CISO role has changed to more of a business-centric, go-to expert for boards concerning cybersecurity risk management (Grossman, 2017). Today, CISOs exist to cultivate safe business practices, changing how the organization conducts business from top to bottom (Institute for Applied Network Security, 2017a). They commonly find themselves in

the role of teacher or change agent, highly responsive to the needs of the organization while demonstrating the value of being operationally involved (Institute for Applied Network Security, 2017a). CISOs are also heavily relied upon to help other executives understand the cyberspace environment, promoting a culture of defense despite the guarantee of pushback from many in the core business elements (Sheridan, 2017). Because of the criticality of the role, some studies convey that upwards of 90% of CISOs report directly to the most senior leadership, with about 50% holding a position directly on the top leadership team (Sweeney, 2016).

Proposition 10: The CISO should have unimpeded structural or procedural access to senior leadership to facilitate cybersecurity-oriented culture change, risk-based decision making, and shaping of the corporate strategy.

The CISO plays a critical role in providing cybersecurity insight and guidance to ensure the overall corporate strategy is fundamentally secure (Sheridan, 2016). To do so, they need visibility into the day-to-day operations of each business unit so they can help implement the risk mitigation objectives set forth by the board (Grossman, 2017). With an enterprise view across silos, CISOs know how to leverage strategic and tactical resources to enhance value for the organization (Grossman, 2017). With a demand to understand strategic objectives so that cybersecurity can align with business goals, it is no longer possible to work in silos (BAE Systems, 2017; Rashid, 2015). However, only a quarter of executives rate their CISO as aware of operational objectives and business needs outside of cybersecurity (Rashid, 2015).

Even if the role of the CISO is starting to formulate in the private sector, the authorities for the position still have room to grow. In the 2015 Role of the CISO

report issued by ThreatTack Security, half of the CEOs surveyed noted that CISOs should be held accountable in the event of the breach (Rashid, 2015). However, only 38% said that CISOs should have the authority to develop the cybersecurity strategy and execute procurement actions for capabilities, a decline of 8% from the previous year (Rashid, 2015). This contrast led one respondent to ponder, "If CISOs do not have visibility into operational plans and strategy, and are not included in decision-making processes, how can they be held responsible for a major security issue?" (Rashid, 2015).

Proposition 11: In designing CISO reporting relationships, organizations should minimize role conflict between the CISO and other executive leaders (CIO, COO, CFO) to facilitate maturation of the cybersecurity program.

On the opposite end of the spectrum, some CISOs have taken their authorities to a whole new level, wielding the cyberspace equivalent of "a badge and a gun" to enforce cybersecurity policies and standards (Jones, 2016). Rather than being the corporate version of law enforcement, many CISO advocate for soft-power roles as "educators, problem solvers, facilitators and influencers" (Jones, 2016).

While the key functions of a CISO varied slightly among the literature in this study, there were three common themes that all CISOs must pursue. The first CISO function is to manage the cybersecurity program (Allen et al., 2015; Boulton, 2016; Jones, 2016). Included in this role is the responsibility for overseeing cybersecurity strategy, governance, policy, and compliance. The second CISO function is to manage the resilience of core business functions within the organization (Allen et al., 2015; Jones, 2016). This includes overseeing the incident response program as well as

maintaining a plan for continuity of operations plan for a breach or catastrophic event. The third, and commonly highlighted as most important, function of the CISO is to manage cybersecurity risk (Allen et al., 2015; Boulton, 2016; Jones, 2016). Effectively managing risk includes guiding business decisions regarding cybersecurity considerations, translating cybersecurity concerns into the corporate language, and ensuring mitigation strategies maintain alignment with the organization's risk tolerance (Allen et al., 2015; Boulton, 2016; Jones, 2016).

A byproduct of the Air Force's Task Force Cyber Secure was the creation of an Air Force-level Chief Information Security Officer (Bender & Bryant, 2016). Although specific roles and responsibilities are still being fleshed out, the Air Force CISO has many of the enterprise-level functions of private sector CISOs, with an additional focus on assuring the Air Force's core missions in and thru cyberspace (Bender & Bryant, 2016). The tactical compliment of the AF CISO is the rebranded wing-level cyberspace operations squadron (Kennedy, 2016). The squadron will provide "wing-level expertise to integrate capabilities in, thru and from cyberspace to accomplish the wing's primary mission from generation through execution" (Kennedy, 2016).

Proposition 12: CISOs should fill a strategic, business-centric role that includes overseeing the cybersecurity program, ensuring core business resilience, and managing cybersecurity risk.

RQ 3: What are the Key Considerations for Creating an Organizational Structure that is Postured for Today's Cybersecurity Challenges?

Structuring the Organization for Cybersecurity

One of the greatest challenges facing the success of CISOs and CIOs is the organizational structure of the business itself (Boulton, 2016). The positioning of a CISO is critical as it directly impacts his or her ability to gain the access and visibility across the major business stovepipes necessary to adequately manage the cybersecurity program (Veltsos, 2017).

Advocates for the traditional organizational structure say that CISO should report only to the CIO because cybersecurity is inextricably linked to IT (Boulton, 2016). Recently, both the CISO and CIO are becoming empowered to veto key enterprise-level decisions if either the IT or cybersecurity considerations warrant such an action (Sheridan, 2016). Additionally, segregation of IT and cybersecurity duties is often too challenging to create separate reporting structures, with 40% of Forbes Global 2000 companies indicating that their CISO reported through the CIO (Westby, 2015). With both IT and cybersecurity expertise is in high demand, and upwards of 80% of the CISO role being technical in nature, there is little room for disparate organizations that operate in relatively similar environments (Boulton, 2016). Few independent CISOs have enough of the limited technical human capital, governance structures, or budgetary resources to ensure protection of critical assets (Institute for Applied Network Security, 2017b).

Proposition 13: When designing CISO reporting relationships, organizations should consider the mutually supportive relationship between IT and cybersecurity.

Proposition 14: IT and cybersecurity expertise are in high demand, and often come from a shared pool of available talent resources for the CIO and CISO. The desire to stand up an independent cybersecurity entity should not constrict the human resources of the CIO, as both IT and cybersecurity functions are mutually supportive in creating competitive advantages for the organization.

Although many organizations retain the CISO in a subordinate role to the CIO, some are migrating away from such a relationship to eliminate tensions between security and operations (Veltsos, 2016). Companies pursuing this route advocate for bolstering cybersecurity without overburdening the CIO and IT department (Boulton, 2016). Traditional CIOs place security as neither the only nor primary objective of their function (Upton, 2015). With the natural tension between cybersecurity and IT, either the CIO or CISO is forced to step on the other's toes when advocating for resources and capabilities to senior leadership (Boulton, 2016). More often than not, cybersecurity is the natural release valve when organizations face a value decision between IT and security (Upton, 2015).

Proponents of an independent CISO cite the role conflict with the CIO in an environment of increased focus on cybersecurity as enough justification to create a separate entity within the business (Boulton, 2016). In many cases, the cybersecurity function is often slow to develop when under the guise of the CIO (Upton, 2015). To increase visibility and influence within the core of the business, advocates propose that the CISO must depart from an IT-centric role and into managing cybersecurity risk (Veltsos, 2017).

Regardless of the reporting structure, the CISO must be able to influence senior leader decision making (Jones, 2016). In that regard, the CISO role must be senior

enough to have access to, and gain the respect of, senior executives and the board (Veltsos, 2016). Such respect is gained by engaging in conversations around cybersecurity risk and the ability to integrate risk considerations into the overall enterprise risk management program (Veltsos, 2017). However, the best way to gain credibility and access to decision makers can vary based on the organizational culture or personalities of the executive leadership team (Jones, 2016).

Proposition 15: When designing CISO reporting relationships, organizations should facilitate the CISO's understanding and participation in the core business functions.

Creating a CISO organization, whether subordinate to the CIO or not, requires a significant investment from the executive leadership team. Standing up the organization with a strategic and outcome-driven approach is better than hastily piecing together spare parts from within the organization (Institute for Applied Network Security, 2017a). Identifying and hiring the right talent requires a significant amount of time and energy to get the appropriate mix of technical skills and business acumen (Sheridan, 2017). Following the most liberal maturity models, five to seven years is a realistic timeframe to build the trust, team, and culture necessary to have a high-functioning CISO-led cybersecurity program (Institute for Applied Network Security, 2017b).

The challenges of structuring the cybersecurity mechanism in the private sector are also present in the public sector. In the aftermath of a high-visibility breach at the Food and Drug Administration, the House of Representatives Committee on Energy and Commerce issued a report on the CIO and CISO structure at the Department of

Health and Human Services (Upton, 2015). Citing the need to elevate the CISO to facilitate maturation of the cybersecurity program, the committee recommended changes to the HHS organizational structure. Figures 4 and 5 represent the organizational structure before the breach occurred and the proposed structure following the congressional report, respectively.

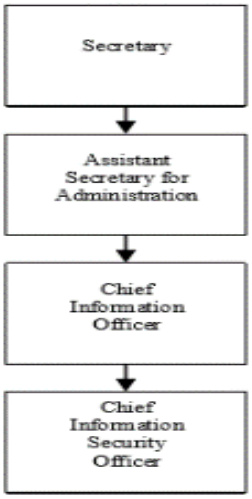


Figure 4. Current Organizational Structure of HHS CIO and CISO (Upton, 2015)

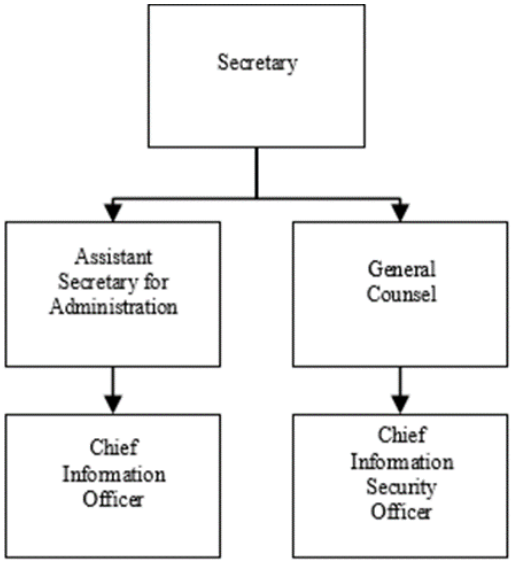


Figure 5. Proposed Organizational Structure of HHS CIO and CISO (Upton, 2015)

Summary

This chapter summarizes the major takeaways from the systematic literature review and identifies relevant themes as they pertain to the research questions, summarized as propositions, for consideration by the reader. Overall, 15 key propositions were identified from the systematic literature review that should serve as considerations for Air Force Major Commands looking to posture their organizational structure for cybersecurity.

IV. Conclusions and Recommendations

Chapter Overview

This chapter examines the conclusions and significance of the research accomplished for this project. Additionally, this chapter includes recommendations for further research in this area.

Conclusions of Research

The analysis performed during this research provides an unbiased perspective to the key considerations for reorganizing MAJCOM staffs for cybersecurity in the Information Age. This includes a total of 15 observations from a systematic literature review that can guide the thinking of Air Force MAJCOMs looking to restructure to confront the ever-increasing challenges of the cyberspace domain:

Proposition 1: The world is becoming increasingly dependent on cyberspace, a domain which is extremely complex, subject to attacks from capable and determined adversaries, difficult to defend, and can cause significant operational and financial losses, if breached.

Proposition 2: Cybersecurity is no longer a technical issue, but one of managing risk.

Proposition 3: Cybersecurity issues should be discussed in the core language of the business.

Proposition 4: Rather than focusing on securing cyberspace capabilities, organizations should emphasize assuring mission dependencies on cyberspace capabilities.

Proposition 5: Leadership should set the conditions for resilience by ensuring the ability to operate through, and rapidly recover from, disruptions to cyberspace dependencies.

Proposition 6: A strong cross-functional cybersecurity governance program should be underwritten by senior leadership as governance provides the framework for the organization's success in cyberspace.

Proposition 7: The senior executive of the organization is the ultimate owner of cybersecurity risk as he or she is accountable if the risk materializes.

Proposition 8: Boards and executive leadership should take an active role in maximizing the effectiveness of the cybersecurity program.

Proposition 9: CIOs should assume the role of a visionary and primary driver of innovation through the implementation of IT solutions that propel the core business forward.

Proposition 10: The CISO should have unimpeded structural or procedural access to senior leadership to facilitate cybersecurity-oriented culture change, risk-based decision making, and shaping of the corporate strategy.

Proposition 11: In designing CISO reporting relationships, organizations should minimize role conflict between the CISO and other executive leaders (CIO, COO, CFO) to facilitate maturation of the cybersecurity program.

Proposition 12: CISOs should fill a strategic, business-centric role that includes overseeing the cybersecurity program, ensuring core business resilience, and the management of cybersecurity risk.

Proposition 13: When designing CISO reporting relationships, organizations should consider the mutually supportive relationship between IT and cybersecurity.

Proposition 14: IT and cybersecurity expertise are in high demand, and often come from a shared pool of available talent resources for the CIO and CISO. The desire to stand up an independent cybersecurity entity should not constrict the human resources of the CIO, as both IT and cybersecurity functions are mutually supportive in creating competitive advantages for the organization.

Proposition 15: When designing CISO reporting relationships, organizations should facilitate the CISO's understanding and participation in the core business functions.

Significance of Research

This research addresses the critical and contentious issue of organizing personnel for cybersecurity challenges in the Information Age. In adapting to such challenges, MAJCOMs have taken varying degrees of action to structure forces to meet the specific needs of their commands. However, many decisions were an urgent response to

manpower reductions rather than forward-looking, mission-related requirements. This body of work provides the MAJCOM staff a consolidated list of key considerations for organizing their workforce to meet the increasing cybersecurity demands of today.

Recommendations for Action

Most MAJCOMs have already taken positive initial action by defining a reporting relationship between the MAJCOM/A6 (CIO equivalent) and the MAJCOM/A3 (COO equivalent) with the goal of bringing cybersecurity concerns into the core operational function of the command.

However, the cybersecurity function at the MAJCOM has matured at a pace consistent with neither the changing threat environment in cyberspace nor industry best practices. Several key programs being implemented at the Headquarters Air Force level might drive the MAJCOMs to reorganize their cybersecurity organizations sooner than later. Such programs include the creation of the Air Force CISO office, the standup of cyberspace operations squadrons at the wing-level, and the mandated use of the NIST framework for mitigating cybersecurity risk. These issues will require extensive MAJCOM involvement to coordinate activities across the enterprise.

Any changes to the cybersecurity program at the MAJCOMs should as a part of a deliberate and calculated strategy, rather than in a hasty or reactive response to the demands of higher headquarters. An immediate recommendation is to stand up a CISO-equivalent organization at the MAJCOM. Establishing a single entity that is responsible for the MAJCOM cybersecurity program is an important step in progressing toward a culture of resilience and mission assurance of the core missions. It is the

recommendation of the researcher that such an organization remain under the purview of the A3 and A6 in order to leverage the operational and technical expertise of both organizations. However, the CISO should have regular procedural access to the MAJCOM Commander or Vice Commander through a robust governance structure to facilitate conversations on the acceptance or mitigation of cyberspace risk.

Furthermore, senior leadership at all levels should continue to increase their involvement in cybersecurity matters so that risk-based decisions can be made at the enterprise level of each MAJCOM to facilitate mission assurance and resilience of the Air Force core missions. Changing to a mission assurance and resilience-based culture will require persistent, top-down engagement from leadership to cement cybersecurity fundamentals in the day-to-day activities of Airmen.

Finally, as the cybersecurity program reaches maturity and the workforce develops over the coming years, the Air Force should consider creating an independent staff element that reports directly to the MAJCOM Commander for all cybersecurity matters. It is the opinion of the researcher that cybersecurity matters will soon outgrow the capacity of any existing staff entity and will require not only the dedicated attention of a directorate-level leader, but the visibility and accountability that comes with structural access to the risk-acceptance authority.

Recommendations for Future Research

This research is strategic manner, with broad references to a generic MAJCOM organizational structure. Further research should be tailored to each MAJCOM to identify mission-specific requirements for its cybersecurity program.

Additionally, a cross-functional study that examines the expertise required to adequately staff the CISO organization from existing Air Force Specialty Codes would be worthwhile. As discussed in this study, cybersecurity is no longer a purely technical issue and will require the involvement of multi-domain and multi-functional expertise to appropriately solve the challenges of the future.

Summary

This chapter examined the conclusions and significance of the research accomplished for this project. Additionally, this chapter included recommendations for action at the MAJCOM level and areas for further research.

Organizing Air Force MAJCOMs for Today's Cybersecurity Challenges

The roles and responsibilities for managing cybersecurity in the Air Force MAJCOMs are inadequate for the challenges of the Information Age. The Air Force could improve its cybersecurity posture to better assure the core missions by adopting industry best practices.

Maj Jonathan French
Advisor: Maj Benjamin Hazen, PhD
Advanced Study of Air Mobility (ENS)
Air Force Institute of Technology

Introduction

The Internet era ushered in an unprecedented wave of cyberspace capabilities that changed the world. It is difficult to find even the smallest part of daily life that is not dependent on some form of information technology.

While cyberspace is ubiquitous in society, so are the multitude of threats that seek to exploit it for gain. Historically speaking, cybersecurity seems to lag the IT sector in producing capabilities needed to secure the advantages of an Information Age world.

The Air Force is not immune to the challenges of cybersecurity, and perhaps is a more lucrative target than many sectors of industry. However, the Air Force's means to approach the cybersecurity problem at the MAJCOM level and above has remained stagnant for nearly a decade. With increasing cyberspace dependencies and their associated threats, it is imperative that Air Force MAJCOMs understand cyberspace risk to their missions and have a means to include it in their operational decision-making. Organizing the structure of the MAJCOM staff to assume an increased role in cybersecurity is an operational imperative for the Air Force to be successful in the Information Age of warfare.

Research Goals

The purpose of this research is to determine key considerations for the restructuring the Air Force MAJCOM staffs to better posture for cybersecurity challenges in the Information Age. This research answers the following questions through a systematic literature review (SLR):

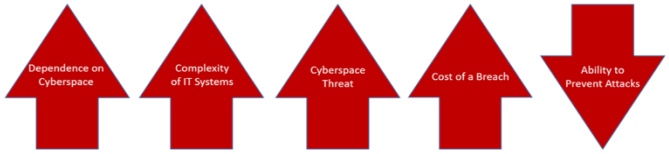
Has the increased cyberspace threat changed the way that industry approaches cybersecurity?

What are the roles and responsibilities of cybersecurity entities in the public and private sector?

What are the key considerations for creating an organizational structure that is postured for today's cybersecurity challenges?

AIR FORCE INSTITUTE OF TECHNOLOGY

Analysis, Conclusions, and Recommendations



Key Findings:

1. The world is becoming increasingly dependent on cyberspace, a domain which is extremely complex, subject to attacks from capable and determined adversaries, difficult to defend, and can cause significant operational and financial losses, if breached.
2. Cybersecurity is no longer a technical issue, but one of managing risk.
3. Cybersecurity issues should be discussed in the core language of the business.
4. Rather than focusing on securing cyberspace capabilities, organizations should emphasize assuring mission dependencies on cyberspace capabilities.
5. Leadership should set the conditions for resilience by ensuring the ability to operate through, and rapidly recover from, disruptions to cyberspace dependencies.
6. The senior executive of the organization is the ultimate owner of cybersecurity risk as he or she is accountable if the risk materializes.
7. CISOs should fill a strategic, business-centric role that includes overseeing the cybersecurity program, ensuring core business resilience, and the management of cybersecurity risk.

Significance

This research addresses the critical and contentious issue of organizing personnel for cybersecurity challenges in the Information Age. In adapting to such challenges, MAJCOMs have taken varying degrees of action to structure forces to meet the specific needs of their commands. However, many decisions were an urgent response to manpower reductions rather than forward-looking, mission-related requirements. This body of work provides the MAJCOM staff a consolidated list of key considerations for organizing their workforce to meet the increasing cybersecurity demands of today.

Methodology

A systematic literature review (SLR) was conducted to answer the investigative questions of this research. A systematic literature begins with identifying an exhaustive list of pertinent literature based upon certain inclusion criteria while also creating exclusion criteria to minimize the amount of irrelevant material gathered. The included material is examined to identify relevant themes as they pertain to the research questions.

Overall, 15 key propositions were identified from the systematic literature review that should serve as considerations for Air Force Major Commands looking to posture their organizational structure for cybersecurity.

Implications

The current organizational structure as well as the roles and responsibilities for cybersecurity entities are hotly debated within the Air Force, with little mutual understanding of the options available to leadership that leverage lessons learned in industry.

This research will identify and recommend best practices for organizing cybersecurity personnel to help MAJCOM staffs understand the costs and benefits of one method over another. Ultimately, the ideal organizational structure depends on the unique requirements of the MAJCOM Commander.

Future Research

This research is strategic manner, with broad references to a generic MAJCOM organizational structure.

Further research should be tailored to each MAJCOM to identify mission-specific requirements for improving the organizational structure of its cybersecurity program.

Additionally, a cross-functional study that examines the expertise required to adequately staff the CISO organization from existing Air Force Specialty Codes would be worthwhile. As discussed in this study, cybersecurity is no longer a purely technical issue and will require the involvement of multi-domain and multi-functional expertise to appropriately solve the challenges of the future.

Bibliography

Allen, J. H., Crabb, G., Curtis, P. D., Fitzpatrick, B., Mehravari, N., & Tobar, D. (2015). *Structuring the Chief Information Security Officer Organization*. https://doi.org/10.13140/RG.2.1.1242.6967

BAE Systems. (2017). *The Intelligence Disconnect*. *Cyber Defence Monitor*. Guildford, England. Retrieved from www.baesystems.com/businessdefence

Bell, R. (2017). Yahoo CEO Loses Bonus Over Security Lapses. *Data Breach Today*, 5. Retrieved from http://www.databreachtoday.com/yahoo-ceo-loses-bonus-over-security-lapses-a-9748

Bender, W. J. (2016). Moving Toward an Information Age Air Force. *CIO Review*, 2–5. Retrieved from http://aerospace-defense.cioreview.com/cioviewpoint/moving-toward-an-information-age-air-force-nid-13812-cid-5.html

Bender, W. J., & Bryant, W. D. (2016). Assuring the USAF Core Missions in the Information Age. *Air & Space Power Journal*, (Fall), 4–8.

Bodeau, D., Graubart, R., & Heinbockel, W. (2013). *Mapping the Cyber Terrain*. Bedford, MA. Retrieved from https://www.mitre.org/sites/default/files/publications/mapping-cyber-terrain-13-4175.pdf

Bohmayr, W. (2017). Insights from Davos: How boards will drive leadership in cyber resilience. Retrieved April 22, 2017, from https://www.linkedin.com/pulse/insights-from-davos-how-boards-drive-leadership-cyber-walter-bohmayr

Boulton, C. (2016). Debate continues over where CISOs sit in the C-suite. *CIO Magazine*, 3. Retrieved from http://www.cio.com/article/3078567/security/debate-continues-over-where-cisos-sit-in-the-c-suite.html

Brasington, H., & Park, M. (2016). Cybersecurity and Ports: Vulnerabilities, Consequences and Preparation. *AUSMARINE*, (February), 23–24.

Bryant, W. D. (2015). Resiliency in Future Cyber Combat. *Strategic Studies Quarterly*, (Winter), 87–107. Retrieved from http://www.dtic.mil/get-tr-doc/pdf?AD=AD1003656

Bryant, W. D. (2016). Mission Assurance through Integrated Cyber Defense. *Air & Space Power Journal*, (Winter), 5–17. Retrieved from http://www.au.af.mil/au/afri/aspj/digital/pdf/articles/2016-Winter/F-Bryant.pdf

Christiansen, J. (2015). *Risk and Its Place in the Ever Changing Role of Security*. *OPTIV Viewpoint*. Denver, CO. Retrieved from https://www.optiv.com/resources/library/risk-and-its-place-in-the-ever-changing-role-of-security/?page=1&searchQuery=&itemsPerPage=0&category=

Christiansen, J. (2016). Cave Man to Business Man, the Evolution of the CISO to CIRO. In *RSA Conference 2016* (p. 28). San Francisco, CA: OPTIV Security. Retrieved from https://www.rsaconference.com/writable/presentations/file_upload/prof-m07-from-cave-man_to-business-man-the-evolution-of-the-ciso-to-ciro.pdf

Cobb, P. (2015). The Ripple Effect of the CISO in the C-Suite. Retrieved April 22, 2017, from https://securityintelligence.com/the-ripple-effect-of-the-ciso-in-the-c-suite/

Department of the Air Force. Cyberspace Operations, AFDD 3-12 (2011). Washington: HQ USAF. Retrieved from https://doctrine.af.mil/download.jsp?filename=3-12-Annex-CYBERSPACE-OPS.pdf

Durach, C. F., Wieland, A., & Machuca, J. a. D. (2015). Antecedents and dimensions of supply chain robustness: a systematic literature review. *International Journal of Physical Distribution & Logistics Management*, *45*(1/2), 118–137. https://doi.org/10.1108/IJPDLM-05-2013-0133

Evans, R. P. (2009). *Control Systems Cyber Security Standards Support Activities*. *Idaho National Laboratory Reports*. Washington, D.C.

Focal Point Data Risk. (2017). *Cyber Balance Sheet: The 2017 Report*. Retrieved from https://focal-point.com/sites/default/files/inline-files/Cyber Balance Sheet Report 2017_1.pdf?submissionGuid=03226690-8b80-45f9-86af-28a6e6a2419e

Fox, D. (2013). Solving The "Cybersecurity Puzzle." *Pipeline & Gas Journal*, (February), 38–45. Retrieved from https://pgjonline.com/2013/02/05/solving-the-cybersecurity-puzzle/

Fox, S. J. (2016). Flying challenges for the future: Aviation preparedness in the face of cyber-terrorism. *Journal of Transportation Security*, *9*(3–4), 191–218. https://doi.org/10.1007/s12198-016-0174-1

Freedman, B. J. (2015). *Cyber Risk Management Guidance for Corporate Directors*. Retrieved from http://www.lexology.com/library/detail.aspx?g=800d6480?500a?424d?839f?68879eb98637

Frodl, M. G. (2012). Pirates Exploiting Cybersecurity Weaknesses in Maritime Industry. *National Defense Magazine*, *96*(702), 22. Retrieved from http://www.nationaldefensemagazine.org/archive/2012/May/Pages/PiratesExploitingCybersecurityWeaknessesinMaritimeIndustry.aspx

Geer, D. E. J., & McClure, S. (2016). *How to Measure Anything in Cybersecurity Risk*. Hoboken, NJ: John Wiley & Sons, Inc.

Goldman, J. (2017). All-Time High of 1 ,093 Data Breaches Reported in U.S. in 2016. Retrieved April 22, 2017, from http://www.esecurityplanet.com/network-security/all-time-high-of-1093-data-breaches-reported-in-u.s.-in-2016.html

Grossman, S. (2017). Talking Cybersecurity From a Risk Management Point of View. Retrieved April 22, 2017, from http://www.darkreading.com/careers?and?people/talking?cybersecurity?from?a?risk?management?point?of?view/a/d?id/1328050 2/14

Groysberg, B., & Cheng, J. Y. (2016). The Political Issues Board Directors Care Most About. *Harvard Business Review*, 2–10.

Hamblen, M. (2017). IT and C-level leaders point fingers at each other over cyber defense. *Computer World*, 1–4. Retrieved from http://www.computerworld.com/article/3167905/security/it-and-c-level-leaders-point-fingers-at-each-other-over-cyber-defense.html

Institute for Applied Network Security. (2017a). *CISO Impact: The 5 Secrets of High-Performing CISOs*. Boston, MA.

Institute for Applied Network Security. (2017b). *CISO Impact Overview Brief*. Boston, MA. Retrieved from https://www.iansresearch.com/insights/ciso-impact

Jones, J. (2016). The Role of Cyber Risk in the Organization. In M. Woodson (Ed.), *Cyber Risk* (pp. 61–82). London, UK: Risk Books.

Kennedy, K. B. (2016). Operating In, Thru, From Cyberspace. In *CORONA TOP 2016* (pp. 1–27). Wright-Patterson Air Force Base, OH.

Knapp, K. J., & Boulton, W. R. (2006). Cyber-warfare Threatens Corporations: Expansion into Commercial Environments. *InfoSec Management Journal*, (Spring), 76.

Kotabe, M. (2005). Global security risks and international competitiveness. *Journal of International Management*, *11*(4), 453–455. https://doi.org/10.1016/j.intman.2005.09.004

Libicki, M. C. (2012). Cyberspace Is Not a Warfighting Domain. *Journal of Law and Policy*, *8*(2), 325–336.

Lohrmann, D. (2014). How Vulnerable Is America's Power Grid? *Public CIO*, *12*(2), 31. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=96213743&site=ehost-live

McKinty, C. (2017). The C-Suite and IT Need to Get on the Same Page on Cybersecurity. *Harvard Business Review*. Retrieved from https://hbr.org/2017/04/the-c-suite-and-it-need-to-get-on-the-same-page-on-cybersecurity

Mollison, A. R. (2015). *Fighting Through a Logistics Cyber Attack*. Air Force Institute of Technology. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a619577.pdf

Moteff, J., Copeland, C., & Fischer, J. (2003). *Critical Infrastructures: What Makes an Infrastructure Critical? Congressional Research Service*. Retrieved from http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA467306&Location=U2&doc=GetTRDoc.pdf

National Association of Corporate Directors. (2017). *Cyber-Risk Oversight*. Washington, D.C. Retrieved from https://www.nacdonline.org/files/FileDownloads/NACD Cyber-Risk Oversight Handbook 2017.pdf

Pritchett, M. D. (2012). *Cyber Mission Assurance: A Guide to Reducing the Uncertainties of Operating in a Contested Cyber Environment*. Air Force Institute of Technology. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a563712.pdf

Rashid, F. Y. (2015). CISOs Challenged in C-Suite: Report. *Security Week*, 3. Retrieved from http://www.securityweek.com/cisos-challenged-c-suite-report

Roesener, A. G., Bottolfson, C., & Fernandez, G. (2014). Policy for US cybersecurity. *Air & Space Power Journal*, *28*(6), 38–54. https://doi.org/10.1017/CBO9781107415324.004

Rosello, A. D., Bodine-baron, E. A., Gierlack, K., Munson, K., Narayanan, A., Pita, J., … Tierney, S. (2014). *What Is the Impact of a Cyber Attack on Air Mobility Command's Logistics Information Technology Systems and Processes?* Santa Monica, CA.

Schulz, A. E., Kotson, M. C., & Zipkin, J. R. (2015). *Cyber Network Mission Dependencies*. Lexington, MA. Retrieved from https://www.ll.mit.edu/mission/cybersec/publications/publication-files/full_papers/2015-Schultz-TR-1189.pdf

Sheridan, K. (2016). CIO-CISO Relationship Continues To Evolve. *DARK Reading*. Retrieved from http://www.darkreading.com/careers-and-people/cio-ciso-relationship-continues-to-evolve/d/d-id/1327226

Sheridan, K. (2017). InfoSec Teams Share Keys to CISO Success. *DARK Reading*, 11. Retrieved from http://www.darkreading.com/careers-and-people/infosec-teams-share-keys-to-ciso-success/d/d-id/1328096

Sweeney, B. (2016). Cybersecurity Is Every Executive's Job. *Harvard Business Review*, 2–5. Retrieved from https://hbr.org/2016/09/cybersecurity-is-every-executives-job

Trump, D. Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (2017). United States of America: White House Homepage. Retrieved from https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

U.S. Joint Chiefs of Staff. (2013). Joint Publication 3-12 Cyberspace Operations. Washington, D.C. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf

Upton, F. (2015). *Information Security at the Department of Health and Human Services*. Washington, D.C. Retrieved from http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/114/Analysis/20150806HHSinformationsecurityreport.pdf

Veltsos, C. (2016). Is Your CISO Out of Place? Retrieved April 22, 2017, from https://securityintelligence.com/is-your-ciso-out-of-place/

Veltsos, C. (2017). Five Ways to Improve the CISO- Board Relationship. Retrieved April 22, 2017, from https://securityintelligence.com/five-ways-to-improve-the-ciso-board-relationship/

Wagner, D., & Disparte, D. (2016). *Global Risk Agility and Decision Making: Organizational Resilience in the Era of Man-Made Risk*. London, UK: Macmillan Publishers Ltd. https://doi.org/10.1057/978-1-349-948604

Westby, J. R. (2015). *Governance of Cybersecurity: 2015 Report*. Atlanta, GA. Retrieved from https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/tech-briefs/governance-of-cybersecurity.pdf

Williams, B. (2015). Cybersecurity ROI: 3 questions to ask about data. Retrieved April 22, 2017, from https://www.linkedin.com/pulse/cybersecurity-roi-3-questions-ask-data-williams-maj-gen-...

Williams, B. (2016a). C'mon, is This as Far as We Have Come? Retrieved April 22, 2017, from https://www.linkedin.com/pulse/cmon-far-we-have-come-brett-williams-maj-gen-usaf-ret-

Williams, B. (2016b). Cyber Education for the Board: How Much Tech is Enough? Retrieved April 22, 2017, from https://www.linkedin.com/pulse/cyber-education-board-how-much-tech-enough-brett

Williams, B. (2016c). Cybersecurity--An Essential Component of Any Business Decision. Retrieved April 22, 2017, from https://www.linkedin.com/pulse/cybersecurityan-essential-component-any-business-brett

Williams, B. (2016d). Executive Cyber Training: Moving From Awareness to Action. Retrieved April 22, 2017, from https://www.trainingindustry.com/leadership/articles/executive-cyber-training-moving-from-awareness-to-action.aspx

Wilson, B. E., Gagnon, G., Blackwell, H., Medgyessy, M., Miller, A., Criswell, B., Oxton, B., Ha, T., Sorenson, D., Elliot, S. (2016). Embedding Airmenship in the Cyberspace Domain: The first few steps of a long walk. *The Cyber Defense Review*, *1*(1), 27–32.

Winnefeld, A. S., Kirchhoff, C., & Upton, D. M. (2015). Cybersecurity's Human Factor: Lessons from the Pentagon. *Harvard Business Review*, (September), 86–95.

World Economic Forum. (2017). *Advancing Cyber Resilience: Principles and Tools for Boards*. New York, NY. Retrieved from http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
15-06-2017	GRP	May 2016 – Jun 2017

4. TITLE AND SUBTITLE
Organizing Air Force Major Commands for Today's Cybersecurity Challenges

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
French, Jonathan M., Major, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 640
WPAFB OH 45433-8865

8. PERFORMING ORGANIZATION REPORT NUMBER
AFIT-ENS-MS-17-J-026

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Mobility Command
Brig Gen Brian Robinson
402 Scott Dr, Unit 3M12
Scott AFB, IL 62225
DSN 779-3315 brian.robinson@us.af.mil

10. SPONSOR/MONITOR'S ACRONYM(S)
AMC/A3

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Distribution Statement A. Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES
This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT
The scope and scale of cyberspace threats has evolved in parallel to the dramatic increase in global dependence on Information Technology (IT) capabilities in the Information Age. However, cybersecurity capabilities continue to lag the threat in fighting for freedom of maneuver and access in the global commons of the Internet. Industry continues to adapt their cybersecurity programs and organizational design to meet these challenges, yet the Department of Defense and military services have struggled to keep pace with the ever-changing threat environment. This research pursues a systematic literature review to analyze the evolving landscape of cyberspace threats, industry best practices for managing cybersecurity programs, and current trends in setting up the required supporting organizational structure. The overall objective of the research is to highlight key areas where Air Force Major Commands could improve processes and organizational structures to posture for cybersecurity challenges in the Information Age.

15. SUBJECT TERMS
CISO, CIO, Cybersecurity, Resilience, Mission Assurance, Cyber Risk Management, CISO Structure

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Hazen, Benjamin T., Maj, PhD, USAF
U	U	U	UU	63	19b. TELEPHONE NUMBER *(Include area code)* (937) 255-6565, x 4337 (Benjamin.hazen@afit.edu)