2014-12

Barriers to cyber information sharing

Harwood, Deanne I.

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

BARRIERS TO CYBER INFORMATION SHARING

by

Deanne I. Harwood

December 2014

Thesis Co-Advisors: John Rollins
Erik Dahl

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 2014	Master's Thesis

4. TITLE AND SUBTITLE
BARRIERS TO CYBER INFORMATION SHARING

5. FUNDING NUMBERS

6. AUTHOR(S) Deanne I. Harwood

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943–5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

As our reliance on the Internet grows, our interconnected networks become more vulnerable to cyberattacks. Cyberattacks and other cyber threats can cause disastrous results, especially if a coordinated targeted attack hits multiple networks at the same time. For this reason, cyber information-sharing among public and private organizations becomes necessary and important to defend our networks. Many cyber threats are difficult to detect and identify by a single organization. Information sharing can help detect these potential risks, prevent cyberattacks, and facilitate incident response to better defend networks. Although the public and private sectors have begun to share cybersecurity information, there are still many barriers that stop agencies from sharing more. This research identifies and reviews what the barriers are to sharing cyber information and possible ways that the barriers can be overcome.

14. SUBJECT TERMS	15. NUMBER OF PAGES
cyber security, cyber information sharing	117
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01–280–5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

BARRIERS TO CYBER INFORMATION SHARING

Deanne I. Harwood
Information Technology Specialist, U.S. Department of Homeland Security
B.S., Strayer University, 1992

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
December 2014

Author: Deanne I. Harwood

Approved by: John Rollins
Thesis Co-Advisor

Erik Dahl, Ph.D.
Thesis Co-Advisor

Mohammed Hafez, Ph.D.
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

As our reliance on the Internet grows, our interconnected networks become more vulnerable to cyberattacks. Cyberattacks and other cyber threats can cause disastrous results, especially if a coordinated targeted attack hits multiple networks at the same time. For this reason, cyber information-sharing among public and private organizations becomes necessary and important to defend our networks. Many cyber threats are difficult to detect and identify by a single organization. Information sharing can help detect these potential risks, prevent cyberattacks, and facilitate incident response to better defend networks. Although the public and private sectors have begun to share cybersecurity information, there are still many barriers that stop agencies from sharing more. This research identifies and reviews what the barriers are to sharing cyber information and possible ways that the barriers can be overcome.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CSC	Advanced Cyber Security Center
APT	Advanced Persistent Threat
CAQDAS	Computer Assisted Qualitative Data Analysis Software
CI	critical infrastructure
CISPA	Cyber Intelligence Sharing and Protection Act
CSA	Cybersecurity Act of 2012
CNCI	Comprehensive Cyber Security Initiative
COMMs ISAC	Communications Infrastructure Information Sharing and Analysis Center
CRS	Congressional Research Services
CYCON	International Conference on Cyber Conflict
DBA	database administrator
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DOJ	Department of Justice
ECS	Enhanced Cybersecurity Services
ENISA	European Network and Information Security Agency
EO	executive order
ESSA	Enhanced Shared Situational Awareness
FAR	Federal Acquisition Regulation
FISA	Foreign Intelligence Surveillance Act
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FS-ISAC	Financial Services Information Sharing and Analysis Center
ICAM	Identity Control and Access Management
ICT	Information and Communications Technology
IOC	indicators of compromise
IODEF	Incident Object Definition
ISA	Information Sharing Agreement
ISP	Internet service provider
NCTC	National Counterterrorism Center
NIST	National Institutes of Standards and Technology
NSA	National Security Agency
NSCS	National Security Council staff
OpenIOC	Indicators of Compromise

PCCIP	President's Commission on Critical Infrastructure Protection
PDD-63	Presidential Decision Directive 63
PDF	portable document format
PPD	Presidential Policy Directive
SSA	Shared Situational Awareness
STIX	Structured Threat Information eXpression
TAXII	Trust Automated eXchange of Indicator Information
TTP	tactics, techniques, and procedures
XML	Extensible Markup Language

EXECUTIVE SUMMARY

Society is increasingly dependent upon the Internet and the systems delivered through it. These systems help ensure that they deliver and maintain essential services in the face of attacks, failures, and accidents. Our critical infrastructure sector is reliant on networked environments for its daily operation. It is these systems that the consumer has come to rely on too in order to do their banking, purchase their goods, and extract money from ATM's when needed. If any of these systems were to fail or be hacked by cyber criminals, the trust that consumers have in these systems will be altered and it would take a long time for the industry to rebuild that trust.

President Obama has declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation" and that "America's economic prosperity in the 21st century will depend on cybersecurity."[1] Our economy and national security depend on a secure cyberspace. One of the pillars of our nation's cybersecurity strategy is to improve our resilience to cyber incidents and to reduce and defend against cyber threats.

An important component of securing our IT infrastructure is the sharing of cybersecurity information between and among private entities. In particular, the sharing of information about cybersecurity threats, such as incident or threat reports, indicators, threat signatures, and alerts (collectively, "cyber threat information") among these entities has the potential to greatly improve the safety of our systems. In his February 2013 Executive Order, the President highlighted the important role the government can play in sharing information with private sector entities, while ensuring that privacy and civil liberties protections are in place.[2]

Today, there are several projects underway where cyber threat information sharing is taking place, both informally and through formal exchange. Further, the sector-

[1] The White House , "National Security Council Cybersecurity," accessed August 1, 2013, http://www.whitehouse.gov/cybersecurity.

[2] Exec. Order No. 13636, 78 C.F.R. 11739 (2013).

specific Information Sharing Analysis Centers (ISACs) have been established to advance the physical and cybersecurity of critical infrastructures and the recently published NIST Cybersecurity Framework is helping to increase sharing capabilities.

There are many ways to share data. It can be structured or unstructured data. It can be shared via automated methods, manually, or both. There are many benefits to sharing cybersecurity related information including an increase in the security, availability, integrity, and efficiency of our information systems which leads to more secure networks.

Given the importance of information sharing, this thesis sets out to examine the barriers to cybersecurity information sharing and how some of these barriers may be overcome. The information in this thesis draws from the review of available literature—both academic and non-academic publications. The findings of this research are a step forward to identify those barriers which are most important and how they may be overcome.

ACKNOWLEDGMENTS

I would like to thank Ms. Wendy Coyle, Mr. Daniel Ritz, and Mr. Brendan Goode of the Network Security Deployment Division, Office of Cybersecurity and Communications, National Protection and Programs Directorate, and Department of Homeland Security for allowing me the time away from the office in order to participate in the Naval Postgraduate School Center for Homeland Defense and Security program.

I also would like to thank my advisors John Rollins and Dr. Erik Dahl of the Naval Postgraduate School. Their guidance and input was instrumental in the completion of my thesis.

I would also like to acknowledge my colleagues in Cohort 1303/1304, who provided their insights and friendship during our distant learning segments and while in residence in Harpers Ferry, WV.

Most importantly, I need to thank my incredibly supportive husband, Doug, and my two daughters, Ashley and Amy, for their support and encouragement. They, and my two dogs, Lexy and Riley, were always by my side.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. INTRODUCTION

After the attacks of September 11, 2001, two commissions concluded that information-sharing is a critical element for preventing terrorist attacks and for protecting the United States. The National Commission on Terrorist Attacks upon the United States (9/11 Commission) concluded that information-sharing had not been a priority for the federal government before the attacks.[1] The Markle Task Force was formed in 2002 to identify best practices in making information discoverable and accessible and enabling improved decision making with regard to threats against our nation. The Task Force found deficiencies in information sharing, and pushed for continued improvements in information sharing.[2]

The need to share data, including cybersecurity information, among federal agencies is imperative. According to Michael Daniel, special assistant to the president and the cybersecurity coordinator, sharing threat information is critical to effective cybersecurity.[3] Reducing barriers to information-sharing is a key element of the Obama administration's strategy to improve the nation's cybersecurity, and the administration is aggressively pursuing these efforts through both executive action and legislation.[4]

Organizations need access to timely cyber threat information in order to detect, respond to, and protect against cyberattacks and cyber threats. Each federal agency has its own networks and data repositories that make it very difficult to piece together information that could collectively serve as a warning. As the White House's 2009

---

[1] National Commission on Terrorist Attacks upon the United States, *The 911 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United State*s, (Washington, DC: U.S. Government Printing Office, 2004), 567.

[2] Markle Foundation Task Force, *Nation at Risk: Policy Makers Need Better Information to Protect the Country* (New York: Markle Foundation, March 2009).

[3] Michael Daniel profile, *The White House Blog*, accessed September 2, 2014, http://www.whitehouse.gov/blog/author/Michael%20Daniel.

[4] Michael Daniel, "Getting Serious about Information Sharing for Cybersecurity," *The White House Blog*, April 10, 2014, http://www.whitehouse.gov/blog/2014/04/10/getting-serious-about-information-sharing-cybersecurity.

Cyberspace Policy Review explained, "Information is key to preventing, detecting, and responding to cyber incidents. A full understanding and effective response may only be possible by bringing information from those various sources together for the benefit of all."[5]

The review identified enhanced information-sharing as a key component of effective cybersecurity, and the administration has made considerable progress in cybersecurity information sharing. For example, through support from the White House Cybersecurity Office within the National Security Council Staff (NSCS), the Comprehensive Cyber Security Initiative (CNCI) initiative number five (#5) connects the National Cyber Operations Centers and provides support for Enhanced Shared Situational Awareness (ESSA).[6] The Department of Homeland Security (DHS) is working to develop the Enhanced Cybersecurity Services (ECS) program to share cyber information with private industry partners.[7] But these endeavors, while facilitating greater cybersecurity information sharing, are just the beginning of this important initiative, and barriers still remain, limiting the ability of organizations to effectively and efficiently share. The barriers that have been noted by government and industry include such things as trust, legal, and technology.

In the cybersecurity community, information-sharing is the act of exchanging cyber threat information between analysts to improve cyber network defenses.[8] Trust between analysts and organizations are critical. Laws need to ensure that the privacy of citizens is upheld when information is exchanged, and the technology must be in place to enable secure machine–to-machine sharing of cybersecurity information.

---

[5] The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, DC: The White House, 2009).

[6] "Comprehensive National Cybersecurity Initiative," The White House, accessed September 9, 2014, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

[7] U.S. Department of Homeland Security, *Privacy Impact Assessment for the Enhanced Cybersecurity Services (ECS)* (Washington, DC: U.S. Department of Homeland Security, 2013).

[8] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar What Everyone Needs to Know* (New York: Oxford University Press, 2014), 222–246.

B. STATEMENT OF THE PROBLEM

Many experts agree that the terrorist attacks of 9/11 were caused, in part, by the inefficiency in the sharing of information.[9] According to the National Strategy for Information Sharing and Safeguarding, "Our national security depends on our ability to share the right information, with the right people, at the right time."[10] There have been many initiatives to enable the sharing of information, such as the creation of the National Counterterrorism Center (NCTC), but the focus has been on terrorism- and law enforcement-related information and not on cybersecurity.[11]

Why is it important to share cybersecurity information? In April 2012, the public disclosure of attempted attacks against natural gas pipeline company systems demonstrated the necessity—and the urgency—of better cyber-security information sharing.[12] The coordinated attacks began in December 2011 but were not recognized and analyzed by the Department of Homeland Security (DHS) until March 2012 because information on these incidents was not reported to DHS in a timely manner.[13] If stakeholders are provided with timely data on the most critical threats, they can use this information to implement an effective solution that will reduce the risk to their mission-essential services.

Furthermore, according to a Government Accountability Office (GAO) report from February 2013, threats to systems supporting critical infrastructure and federal

---

[9] Amy B. Zegart, *Spying Blind: The CIA, the FBI, and the Origins of 9/11* (Princeton, NJ: Princeton University Press, 2009).

[10] The White House Office, *National Strategy for Information Sharing and Safeguarding* (Washington, DC: The White House, December 2012).

[11] Richard A. Best, Jr., *The National Counterterrorism Center (NCTC)—Responsibilities and Potential Congressional Concerns* (CRS Report No. R41022) (Washington, DC: Congressional Research Service, 2011).

[12] Mark Clayton, "Alert: Major Cyber Attack Aimed at Natural Gas Pipeline Companies," *Christian Science Monitor*, May 5, 2012, http://www.csmonitor.com/USA/2012/0505/Alert-Major-cyber-attack-aimed-at-natural-gas-pipeline-companies.

[13] Bipartisan Policy Center Cybersecurity Task Force, *Cyber Security Task Force: Public-Private Information Sharing* (Washington, DC: Bipartisan Policy Center, 2012), 5–6.

operations are evolving and growing.[14] Federal agencies report an increase in the numbers of cybersecurity incidents that have placed sensitive information at risk, with potentially serious impacts on federal and military operations; critical infrastructure; and the confidentiality, integrity, and availability of sensitive government, private sector, and personal information.[15] The increasing risks are demonstrated by the dramatic increase in reports of security incidents, the ease of obtaining and using hacking tools, and steady advances in the sophistication and effectiveness of attack technology.[16]

Information-sharing, timely analysis and warnings continue to challenge efforts to detect, respond to, and mitigate cybersecurity incidents, even though improvements in cybersecurity information sharing have become a higher priority. There are significant barriers that are impeding the progress of a more complete information-sharing approach. Most experts agree that there are vast benefits with sharing cybersecurity information and that the barriers must be addressed. In a recent book, for example, P.W. Singer and Allan Friedman of the Brookings Institution write that the key benefit of information-sharing is that it allows a more complete view of emerging threats and patterns.[17] They point out that it arms analysts with the lessons learned from other analysts' experiences. Beyond empowering the decision makers, information-sharing also benefits organizations and analysts by supporting the diffusion of experience and best practices of each organization.[18]

C. BACKGROUND

In recent years, cyber exploitation and malicious activity are becoming increasingly sophisticated, targeted, and serious. The 2013 Internet Security Threat Report by Symantec Corporation identified a 42% increase in targeted attacks from

---

[14] Government Accountability Office, *Cybersecurity National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented* (GAO-13-187) (Washington, DC: Government Accountability Office, February 2013).

[15] Ibid., 10.

[16] Ibid.

[17] Singer and Friedman, *Cybersecurity and Cyberwar*, 222–246.

[18] Ibid.

2012.[19] In addition, there were over 5,000 new vulnerabilities identified in 2013.[20] Of the new vulnerabilities, 415 were on mobile operating systems and 69% were email vulnerabilities that were delivered to inboxes as spam.[21] One in 400 of the spam emails were identified as phishing emails, and 1 in 300 were identified as viruses.[22]

According to experts at the Center for Strategic and International Studies, the greatest threat that DHS must defend against in the coming years will come not from a physical opponent, but from cyberspace.[23] This threat will only continue to grow as our reliance on technology continues to evolve at a rapid rate and state and non-state actors increasingly invest in cyber capabilities. The danger posed by cyberattacks extends not only to critical infrastructure systems such as the power grid and water systems but also to the nation's economy. Equally, if not more, worrying than the potential for a catastrophic "cyber Pearl Harbor," as described by former Defense Secretary Leon Panetta, is the ongoing theft of intellectual property from U.S. corporations and businesses.[24] As noted by General Keith Alexander, former commander of United States Cyber Command and director of the National Security Agency, intellectual property theft represent "the greatest transfer of wealth in history." This theft not only leeches billions of dollars from the nation's economy each year, but also grants potential adversaries access to sensitive information regarding U.S. technologies, including those related to national security. According to the Center for Strategic and International Studies (CSIS), one of DHS' greatest challenges in the coming years will be to protect against these attacks and intrusions. In doing so, DHS must establish enhanced systems for improved intelligence and information-sharing.[25]

---

[19] Symantec Corporation, *2013 Internet Security Threat Report* (Mountain View, CA: Symantec, 2013).

[20] Ibid.

[21] Ibid.

[22] Ibid.

[23] Rick Nelson and Rob Wise, "Homeland Security at a Crossroads: Evolving DHS to Meet the Next Generation of Threats," Center for Strategic and International Studies, February 1, 2013, http://csis.org/publication/homeland-security-crossroads-evolving-dhs-meet-next-generation-threats.

[24] Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *New York Times*, October 11, 2012.

[25] Nelson and Wise, "Homeland Security at a Crossroads."

The Federal Financial Institutions Examination Council (FFIEC) recently warned of the threat of rising cyber-attacks within the financial services critical infrastructure sector.[26] These attacks target bank websites and cash machines, prompting a rise in denial-of-service attacks that sometimes are a cover for criminals committing fraud. The council urged the industry to put proper measures in place to guard against this type of fraud. It described one recent case in which criminals stole $40 million from just 12 accounts—far exceeding the actual balance held by clients—in a sophisticated scheme known as an "unlimited operations" fraud.[27]

In addition to these threats, another threat called the Advanced Persistent Threat (APT) has been spreading across government and defense contractor networks. Mandiant Corporation published the Mandiant APT report in March 2013. This report describes the nature of the APT threat and where it is originating.[28] The report analyzes hundreds of investigations that signal that the groups conducting these security breaches around the world are based primarily in China.

Cyber threat information from these types of threats is what stakeholders need in order to implement effective solutions that will reduce the risk to mission-essential services and data. Organizations currently employ their own defensive measures to protect their network infrastructures. With the emergence of a wide variety of sophisticated cyber threats, this has made these disconnected efforts a liability. To prevent the sophisticated adversary, the baseline security posture of the entire organization should be unified through the improved information-sharing of relevant and actionable cyber threat information. In order to do this, experts agree that organizations need to reach out and partner with both private industry and federal organizations and

---

[26] Federal Financial Institutions Examination Council (FFIEC), *Cyber-Attacks on Financial Institutions' ATM and Card Authorization Systems (*Washington, DC*:* Federal Financial Institutions Examination Council, April 2, 2014).

[27] "Financial Regulators Release Statements on Cyber-Attacks on Automated Teller Machine and Card Authorization Systems and Distributed Denial of Service Attacks," FFIEC (Federal Financial Institutions Examination Council), April 2, 2014, http://www.ffiec.gov/press/pr040214.htm.

[28] Mandiant, *APT1 Exposing One of China's Cyber Espionage Units* (Alexandria, VA: Mandiant, 2013).

share threat information, enhance their cyber situational awareness, and protect their networks.[29]

1. The Cyber Threat

Network risks stem from cybercrime, threats from inside the organization, threats to critical infrastructure, and threats from nation state actors that steal information for economic gain.[30] Cybercrime and cyberattacks are genuine threats. Reports of data breaches, hacks, or thefts have become daily news.[31] Therefore, the data about the adversaries and threats are the critical and must be shared.

In recent years, cyber exploitation and malicious activity in the United States are becoming increasingly sophisticated, targeted, and serious.[32] The 2014 U.S. State of Cybercrime Survey found that American businesses and institutions are failing to meet the cybersecurity threats posed by hackers at home and abroad.[33] According to the report, it is clear that the cybersecurity programs of U.S. organizations do not rival the persistence, tactical skills, and technological prowess of their potential cyber adversaries.

Today, common criminals, organized crime rings, and nation-states leverage sophisticated techniques to launch attacks that are highly targeted and difficult to detect. In fact, the U.S. Director of National Intelligence has ranked cybercrime as the top national security threat, higher than that of terrorism, espionage, and weapons of mass destruction.[34] The report also found that in a volatile cybercrime environment, attackers continually and rapidly update their tactics to maintain an advantage over any security

---

29 Singer and Friedman, *Cybersecurity and Cyberwar*, 222–246.

30 *Cyber Attacks: An Unprecedented Threat to U.S. National Security House of Representative: Hearing before Subcommittee on Europe, Eurasia, and Emerging Threats of the Committee on Foreign Affairs*, 113th Cong., 2, 1, (2013).

31 Steven Titch, "U.S. Cybersecurity Policy: Problems and Principles," The Heartland Institute, August 1, 2013, http://heartland.org/policy-documents/us-cybersecurity-policy-problems-and-principles.

32 Kevin Mickelberg, Neal Pollard and Laurie Schive, *2014 U.S. State of Cybercrime*, London: PricewaterhouseCoopers, June 2014. http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf.

33 Mickelberg, Pollard and Schive, *2014 U.S. State of Cybercrime*.

34 *Current and Future Worldwide Threats to the National Security of the United States, Remarks Delivered to the Senate Armed Services Committee* (2014) (statement of James R. Clapper, director of National Intelligence).

safeguard such as anti-virus protection. Recently, for instance, hackers engineered a new round of distributed denial of service (DDoS) attacks that can generate traffic rated at a staggering 400 gigabits per second, the most powerful DDoS assaults to date.[35]

One of the most recent and high profile attacks was the November 2013 Point of Sale (POS) attack on Target Corporation. A cyberattack compromised up to 40 million payment cards during the first three weeks of the holiday shopping season.[36] The malware was used in conjunction with a variety of other tools, and the criminals displayed a high degree of skill in orchestrating the various components of the breaches.[37]

Financially motivated cyber criminals have used POS malware at an accelerating pace for several years. POS malware that includes memory-scraping capabilities has been available for some time.[38] The malicious software that enabled hackers to steal information from credit and debit cards from November 27 to December 15 was later found on 25 additional checkout machines and continued to collect shoppers' information for three more days.[39] On December 27, Target also acknowledged, contrary to early reports, that personal identification numbers to debit and credit cards were also exposed. During the process of this attack, Target remained operational both through its brick-and-mortar stores as well as its website.

The Target case is indicative of growing threat of cyberattacks. It is important to understand the vulnerabilities locally and globally, and how other governments respond to these kinds of attacks.

---

35 Mickelberg, Pollard and Schive, *2014 U.S. State of Cybercrime*, 21.

36 Department of Homeland Security (DHS), National Cybersecurity and Communications Integration Center (NCCIC), United States Secret Service (USSS), Financial Sector Information Sharing and Analysis Center (FS-ISAC), and iSIGHT Partners. *POS Malware Technical Analysis: Indicators for Network Defenders* (Washington, DC: Department of Homeland Security, January 16, 2014.)

37 DHS, NCCIC, USSS, FS-ISAC and iSight, *POS Malware Technical Analysis.*

38 Ibid.

39 Michael Riley et al., "Target Missed Warnings in Epic Hack of Credit Card Data," *Business Week*, March 13, 2014, http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

To defend against threats, cybersecurity analysts and leaders must assess the risks they face. Herbert Lin, the chief scientist for Computer Science at the National Academies and one of the leading experts in the field of cybersecurity, explains that the threat is evaluated on three basic factors: "The feasibility of adversaries being able to identify and exploit your vulnerabilities, the effect that would happen if they were able to take advantage of these vulnerabilities, and finally, the likelihood that they will, in fact, be willing to do so."[40]

There is general consensus among practitioners that systems and networks are inherently vulnerable, and they offer a wide array of opportunities for criminal or cyber terrorist organizations to exploit these intrinsic weaknesses.[41] Cybersecurity analysts have long tried to get ahead of the adversaries, principally by analyzing the cyber threat information that is provided to them through such means as cyber threat websites and trusted partners through the sharing of information.

Singer and Friedman insist that the approach to sharing must be about the data.[42] They assert that many things can happen, but someone must cause them. Threats should be assessed by understanding potential bad actors, what they are trying to do, and why. They suggest that when sharing, information stakeholders ask questions such as what type of indicators are we sharing from the cyber information, where did it originate from, and when did it occur? These types of questions could provide answers to more actionable information that can be shared.

Cybersecurity experts refer to this data as "cyber threat intelligence."[43] This is a key part of an organization's defense against cyber adversaries. Examples of cyber threat intelligence include understanding and characterizing such information as what sort of attack actions have occurred or are likely to occur; how can these actions be detected and

---

[40] Seymour E. Goodman and Herbert S. Lin, eds., T*oward a Safer and More Secure Cyberspace* (Washington, DC: The National Academies Press, 2007).

[41] Sylvester Ngoma, "Vulnerability of IT Infrastructures: Internal and External Threats," Congo Vision, accessed September 13, 2014, www.congovision.com/IT-Security-Pub.pdf, congovision.com.

[42] Singer and Friedman, *Cybersecurity and Cyberwar*, 222–246.

[43] Mitre, "Structured Threat Information eXpression—STIX. A Structured Language for Cyber Threat Intelligence Information," accessed December 2, 2013, http://measurablesecurity.mitre.org/docs/stix-intro-handout.pdf .

recognized; how can they be mitigated; who are the relevant threat actors; what are they trying to achieve; what are their capabilities, in the form of tactics, techniques, and procedures they have leveraged over time and are likely to leverage in the future; what sort of vulnerabilities, misconfigurations, or weaknesses they are likely to target; what actions have they taken in the past; etc.[44]

2. National Sharing Initiatives

The Obama administration has launched several initiatives, including the Comprehensive National Cybersecurity Initiative Priority Number-5 (CNCI-5) for enhanced situational awareness of the federal cyber centers, Executive Order (EO) 13636 for Improving Critical Infrastructure Cybersecurity, and Presidential Policy Directive (PPD-21), which is a companion to the EO.[45] CNCI-5 was created to connect current cyber operations centers to enhance situational awareness. Out of this effort came the Enhance Shared Situational Awareness (ESSA) initiative that will provide the real-time cybersecurity situational awareness to improve the security of the U.S. government and U.S. critical infrastructure. Through this initiative the federal cybersecurity centers agreed to an information sharing framework, and shared situational awareness (SSA) requirements to facilitate development and implementation of the ESSA Information Sharing Architecture (ISA).[46]

According to a report by the GAO in 2010, the CNCI-5 could do a better job addressing international efforts by improving cooperation between cybersecurity and law enforcement professionals in different nations, developing security standards, and pursuing international agreements on engagement and information sharing.[47] As of today,

---

44 Ibid.

45 "Fact Sheet: Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience," Department of Homeland Security, March 2013, http://www.dhs.gov/publication/fact-sheet-eo-13636-improving-critical-infrastructure-cybersecurity-and-ppd-21-critical.

46 Office of the Director of National Intelligence, *Information Sharing Environment 2014 Annual Report to the Congres*s (Washington, DC: Office of the Director of National Intelligence, 2014) http://www.ise.gov/annual-report/section4.html.

47 Government Accountability Office, *Cybersecurity: Progress made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative* (GAO 10–338) (Washington, DC: Government Accountability Office, 2010).

the initiative is making great strides in the areas of developing standards, but the focus is still on connecting federal cyber centers and not on national or international cyber operations centers.[48]

There are other initiatives that are working to provide information to only Internet service providers (ISPs) and Defense Industry Board (DIB) partners.[49] Although these systems are working to solve part of the problem, there is still a gap in sharing this information to organizations that do not have the proper clearance level, such as the private sector community as well as the general public. One such system is the Enhanced Cybersecurity Services (ECS) initiative that is supposed to expand the number of companies that receive classified or top secret information from the government about real or potential threats.[50] The problem with this initiative is that to date, few companies have decided to make the investment. ECS is a voluntary program and the government does fund it. Businesses must decide if it makes sense to invest in a secure facility and in network upgrades to handle classified data.[51]

In addition to the CNCI-5 efforts, the EO expands information-sharing and collaboration between the government and the private sector, and establishes a process for identifying critical infrastructure (CI) with high priority for protection.[52] It requires National Institutes of Standards and Technology (NIST) to lead in the development of a framework of cybersecurity standards and best practices for protecting CI and requires regulatory agencies to establish requirements to address the risks. The companion PPD-

48 "Meeting Minutes," Information Security and Privacy Advisory Board, accessed September 2, 2014, http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2013-12/ispab_meeting_minutes_december2013.pdf.

49 Milton Mueller and Andreas Kuehn, "Einstein on the Breach: Surveillance Technology, Cybersecurity and Organizational Change," paper Presented the 12th Workshop on the Economics of Information Security (WEIS 2013),Georgetown University, Washington, DC, June 11–12, 2013.

50 Department of Homeland Security (DHS), *Privacy Impact Assessment for the Enhanced Cybersecurity Services*, Washington, DC: DHS, January 16, 2013.

51 Jason Miller, "DHS Finds Classified Cyber Sharing Program Slow to Take Off," accessed October 5, 2013, http://www.federalnewsradio.com/index.php?nid=851&sid=3356694.

52 "Presidential Policy Directive—Critical Infrastructure Security and Resilience," The White House, February 21, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

21 revises other aspects of policy relating to CI security with the aim of improving integration and efficiency, among other goals.[53]

According to the National Infrastructure Advisory Council, having national unity of effort to strengthen and maintain a secure, functioning, and resilient infrastructure requires broad participation, collaboration, and trust.[54] The council intends to measure the effectiveness of the EO and PPD work by utilizing metrics that were developed by the Homeland Security Studies and Analysis Institute.[55] Future research can include the review of these metrics as these initiatives are put into operation.

According to the White House, there are many companies who are already sharing information on cyber threats with each other and with the government through programs that preserve the privacy of Americans, maintain appropriate constraints on government access to private information, and do not lead to anti-competitive practices.[56] For example, during the denial-of-service attacks that targeted the websites of many leading U.S. banks over the last few years, the Financial Services Information Sharing and Analysis Center coordinated with banks to exchange information to manage the attacks.[57] Also, Boston's Advanced Cybersecurity Center, the Bay Area Security Council, and ChicagoFirst have built smaller trust networks. The White House continues to work with partners in industry to encourage information sharing partnerships and to take to further reduce barriers to information sharing.[58]

---

53 "Presidential Policy Directive—Critical Infrastructure Security and Resilience."

54 "Executive Order and PPD-21 Working Group Recommendations for Maximum Engagement Including the Cybersecurity Framework, in Reducing Cyber Risks to Critical Infrastructure," National Infrastructure Advisory Council, September 4, 2013, http://www.dhs.gov/sites/default/files/publications/WG%20Adoption%20Recomendations.pdf.

55 Matthew H. Fleming and Eric Goldstein, *Metrics for Measuring the Efficacy of Critical-Infrastructure-Centric Cybersecurity Information Sharing Efforts* (Washington, DC: Homeland Security Studies and Analysis Institute, 2012).

56 Michael Daniel, "Getting Serious about Information Sharing for Cybersecurity."

57 *Data Security: Examining Efforts to Protect Americans' Financial Information Hearing Before the House Committee on Financial Services, Subcommittee on Financial Institutions and Consumer Credit,* 113th Cong., 2nd Sess (2014) (statement of William Noonan, USSS Criminal Investigative Division Deputy Special Agent in Charge). https://www.dhs.gov/news/2014/03/05/written-testimony-usss-house-financial-services-subcommittee-financial-institutions.

58 Ibid.

D. PURPOSE OF THE STUDY

This thesis argues that overcoming the barriers to cyber threat information-sharing will help protect American networks from cyberattacks. It addresses barriers tied to trust, technology and law, identifies recent technological advances, and examines ways to overcome the barriers. Furthermore, this thesis reviews the federal cybersecurity information-sharing initiatives and how they may or may not be making progress, as well as the efficacy of emerging standards and technology for cybersecurity information-sharing.

E. RESEARCH QUESTIONS

This research explores the questions, what are the primary barriers to cyber information sharing between government and private sector organizations? And, how can these barriers be overcome? The intent of this research is to help inform policy makers about the problems that prevent better sharing of cybersecurity information and make our cyber information more secure.

To examine these questions, this thesis uses a qualitative method of analysis tool known as NVivo and observational evaluation to identify the strengths and weaknesses of cybersecurity information-sharing with an emphasis on those already identified by government and industry.

Literature sources, such as government documents, books, and websites, were used to perform this study. The literature sources were imported into a software product called NVivo version 10 and thematically coded and analyzed to find emerging themes. NVivo is a Computer Assisted Qualitative Data Analysis Software (CAQDAS) tool that was developed by QSR International.[59] CAQDAS tools are used to assist in identifying patterns and relationships and to interpret the data. This analysis provides further review and evidence of the question on what the barriers are to cybersecurity information-sharing. The process of the research plan for using the software for the analysis is described in Figure 1. Handling qualitative data tends to be an iterative process whereby

[59] "Using NVivo for Qualitative Research," QSR International, accessed June 30, 2014, http://help-nv10.qsrinternational.com/desktop/concepts/using_nvivo_for_qualitative_research.htm.

the process of the research contains the steps for exploring, coding, reflecting, and taking memos. The process is repeated by coding more, querying the data, and so on. This will be further described in Chapter III.

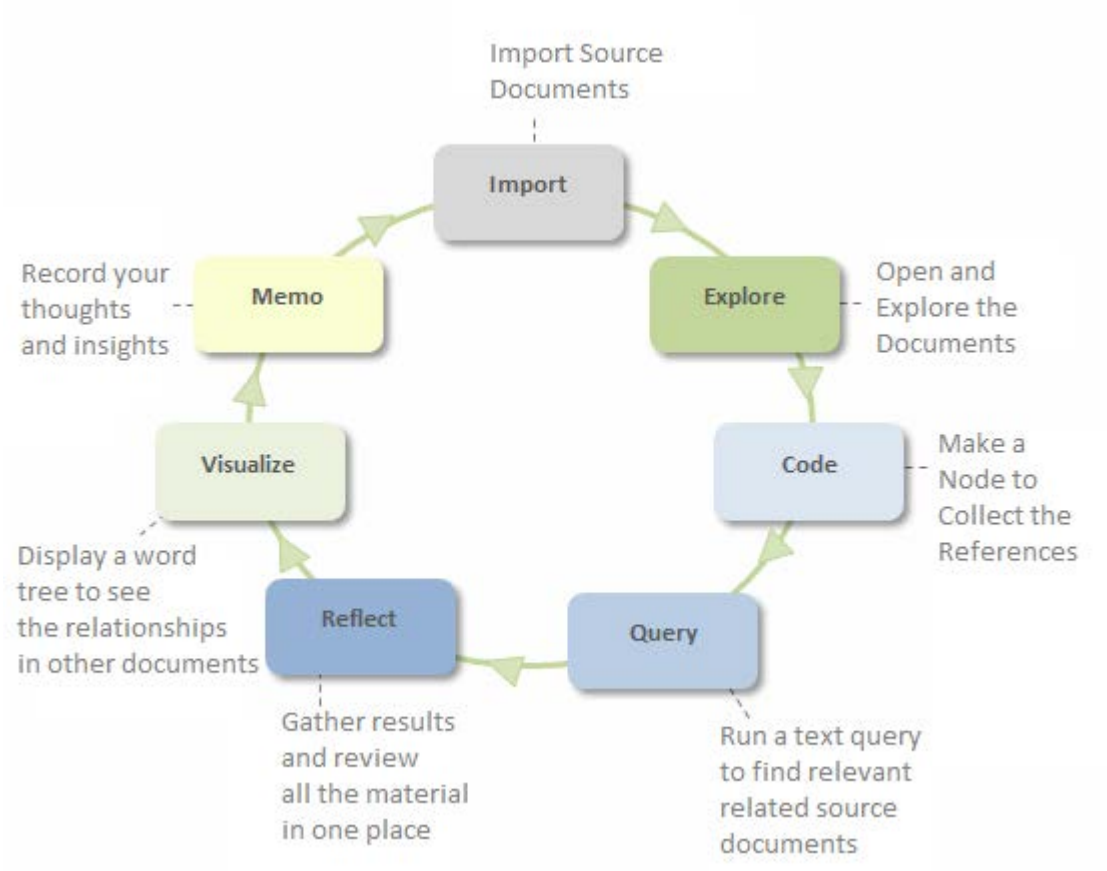

Figure 1. Research plan[60]

In her book, *How to Write a Master's Thesis*, Bui describes how tools such as NVivo, HyperRESEARCH, and HyperTRANSCRIBE are often used to help code and analyze qualitative data.[61] CAQDAS tools such as NVivo have been used in previous research at Naval Postgraduate School. For example, Leslie Sekerka, Roxanne Zolin, and Cary Simon used NVivo software to assist with theme development and facilitate coding

[60] Ibid.

[61] Yvonne N. Bui, *How to Write a Master's Thesis* (Thousand Oaks, CA: SAGE, 2013).

in their 2005 thesis, "Rapid Transformation in a Dual Identity Defense University."[62] In 2013, Tiffany Smythe used NVivo to develop a report on a study of the response to Hurricane Sandy. The software and the coding helped her identify text relevant to the research question of what plans were in place prior to the hurricane and to identify lessons learned.[63]

In addition, there have been research projects in other universities that utilized the NVivo software to help with research. For example, Caroline Bartle of the University of West England utilized NVivo to develop her doctoral thesis on "Spreading the Word: A Social-Psychological Exploration of Word-of-Mouth Traveler Information in the Digital Age." Bartle used a thematic analysis of website contributions, questionnaire responses and interviews, and applied the NVivo software to code from these sources.[64]

Another example of the use of the software was from Xiao Fu of Durham University. Fu used the software in his thesis, The Influences of Budgetary System in a Selection of Large Chinese Companies in the Industry of Electronic Household Appliances," to study companies' everyday business activities. The author reviewed budgetary systems, the relationships that can be discovered between employees' concepts and behaviors concerning them, and the reasons behind these. By answering these questions, Fu found that when you look into Chinese companies' budgetary practices, the understanding provided by Western budgetary studies were relevant. To perform the research, Fu used NVivo to code the data, group the data until clues, threads, relationships, reasons, and answers became evident.[65]

---

[62] Leslie E. Sekerka, Roxanne Zolin and Cary Simon, *Rapid Transformation in a Dual Identity Defense University* (Monterey, CA: Naval Postgraduate School, 2005).

[63] Tiffany C. Smythe, *Assessing the Impacts of Hurricane Sandy on the Port of New York and New Jersey's Maritime Responders and Response Infrastructure* (Boulder, CO: Natural Hazards Center, 2013).

[64] Caroline Bartle, "Spreading the Word: A Social-Psychological Exploration of Word-of-Mouth Traveler Information in the Digital Age," master's thesis, University of the West of England, 2011, http://www2.uwe.ac.uk/faculties/FET/Research/cts/projects/reports/bartle_2011_thesis.pdf.

[65] Xiao Fu, "The Influences of Budgetary System in a Selection of Large Chinese Companies in the Industry of Electronic Household Appliances" (master's thesis, Durham University, 2012) http://etheses.dur.ac.uk/3644/1/Xiao_Fu_Upload_Thesis.pdf?DDD2+.

The rest of the thesis will proceed as follows. Chapter II is the literature review and provides an overview of the problem and the barriers to cyber information-sharing. Chapter III explains how the analysis was performed. In this case, the software tool called NVivo was used to do a qualitative analysis of the literature sources. Chapter IV, the results, covers what was found as the results of the question in the research. Finally, Chapter V provides a discussion of the results and recommendations.

F. LIMITATIONS

As previously discussed, this study encompasses the barriers to cybersecurity information sharing to include policies, legal issues, trust as well as other shortcomings in areas such as technology. The quality of the findings of this study is limited to an evaluation of qualitative information obtained from literature sources. There was no formal survey or interviews from direct sources for this study.

II. LITERATURE REVIEW

A. INTRODUCTION

This literature review addresses research related to the barriers of cyber information-sharing between government and private sector organizations. Although there are some projects identified that are in the process of developing systems to improve cyber threat information-sharing, there are still considerable factors that are making it hard to share more. The review of these factors will provide insight in order to overcome these barriers for a more successful approach.

B. ANALYSIS

Experts note that the private sector has difficulty in sharing its cyber threat indicators and incidents with the government.[66] This is especially true when a cyber incident would threaten the livelihood of that corporation.[67] For instance, if an incident reveals that the company's customers are vulnerable due to the incident, the sharing of the information could hold the company liable therefore, the company is reluctant to share it.[68] Problems like this are just one example of the barriers to sharing cyber information. These problems date back to the beginning of networked systems and when cybersecurity breaches began.

More than ten years ago, an expert from Symantec Corporation identified three specific impediments that hinder cybersecurity information-sharing in the United States: lack of trust, concerns over the protection of shared information, and failure by the government to share their threat information in return.[69] Just last November, Phyllis Schneck, deputy under secretary for cybersecurity for the National Protection and

66 David Sutton, "The Issue of Trust and Information Sharing and the Question of Public Private Partnerships," in *Critical Information Infrastructure Protection and Resilience in the ICT Sector* (Hershey, PA: IGI Global, 2013), 258–276.

67 Sutton, "The Issue of Trust and Information Sharing, 258–276.

68 Ibid.

69 Adam Rak, "Information Sharing in the Cyber Age: A Key to Critical Infrastructure Protection," *Information Security Technical Report* 7, no. 2 (June 2002).

Programs Directorate of the U.S. Department of Homeland Security, spoke about some of same impediments that are still identified as problems to cyber information-sharing.[70] For this reason, it is important to find out why the impediments endure and what can be done to fix them.

There have been many studies done on collaborative sharing of information and trust. For example, in a study done by the European Network and Information Security Agency (ENISA), it was noted that formal means for sharing information should be set up in order to improve the protection and rapid restoration of infrastructure critical to the reliability of communications within and throughout Europe.[71] In a different study by Mitre Corporation, it was determined that information and communication technologies (ICT) are increasingly intertwined across the economies and societies of developed countries.[72] Protecting these technologies from cyber threats requires collaborative relationships for exchanging cyber defense information and an ability to establish trusted relationships.[73]

Scholars identify cyber information as an asset of knowledge. The development of these knowledge assets and protection of them are both complementary and competing concerns for an organization. Each has specific issues related to trust that need to be understood and addressed before an organization is willing to share them.[74]

In the book *Collaborative Computer Security and Trust Management*, the authors suggest an attitude among scholars whereby knowledge assets should be collected and then shared among practitioners, fully leveraging their impact. There is an implicit assumption that all network partners are trustworthy, both individuals and organizations,

---

70 Brandan Blevins, "Experts Propose Better Cybersecurity Information-Sharing Models," *Search Security*, November 14, 2013, http://searchsecurity.techtarget.com/news/2240209036/Experts-propose-better-cybersecurity-information-sharing-models.

71 Neil Robinson and Emma Disley, *Incentives and Challenges for Information Sharing* (Heraklion, Greece: European Network and Information Security Agency, 2010).

72 D. Fernandez Vazquez et al., "Conceptual Framework for Cyber Defense Information Sharing within Trust Relationships" presented at the 2012 4th International Conference on Cyber Conflict, Tallinn, Estonia, June 5–8, 2012.

73 Ibid.

74 Jean-Marc Seigneur and Adam Slagell, eds., Collaborative Computer Security and Trust Management (Hershey, PA: Information Science Reference, 2009), 1–11.

and that fuller distribution of knowledge is always better.[75] The book indicates that this is not always the case and further exploration of this subject area will identify why.

According to experts at the School of Information Sciences and Technology at the Pennsylvania State University, the primary reason for the hesitation to share sensitive information among agencies is a lack of trust.[76] They discuss conflict of interests and turf battles between agencies, and assert that the problem can cause substantial deficiencies. They conclude that existing secure information sharing technologies and protocols cannot provide enough incentives for government agencies to share information with one another without jeopardizing their own interests.[77]

When multiple stakeholders are involved in collaboration, it is typical for their priorities to differ, or even conflict, with one another. In today's increasingly networked world, cybersecurity collaborations may span organizations and countries. There are items identified that may lead to more trusting cybersecurity information-sharing and collaboration.[78] For example, the European Network and Information Security Agency (ENISA) published a paper on cyber information-sharing and found that the most popular structure to facilitate this sharing is a trusted' forum or platform where private sector infrastructure owners or operators can meet face-to-face at regular intervals and hold informal, un-attributable discussions.[79]

Researchers from MITRE Corporation and ISDEFE, a defense and security firm from Spain, published a report for the 2012 4th International Conference on Cyber Conflict (CYCON). They used the ENISA processes and documents to identify four aspects of cyber defense collaboration and improvements to cyber information-sharing. According to the report, there is a long history across the cyber defense community of establishing information-sharing repositories, creating data exchange standards, and

---

75 Ibid.

76 Peng Liu and Amit Chetal, "Trust-Based Secure Information Sharing between Federal Government Agencies," Journal of the Association for Information Science and Technology, no. 56 (2005): 283–298.

77 Liu and Chetal, "Trust-Based Secure Information Sharing," 283–298.

78 Seigneur and Slagell, *Collaborative Computer Security*, 1–11.

79 Ibid.

finding that the repositories were underutilized.[80] They found that in relation to the field of cybersecurity, the debate is about the data types that are useful, what data can be shared due to policies, what models to use to share, and how to address privacy and security.

This thesis will include a study of the legal barriers to cybersecurity information-sharing. Without legal protection, corporations worry that information they share may be used as evidence by the government or in litigation that might come back to haunt them.[81] There have been groups that have asked Congress for legal protection prior to participating in any federal programs. Possible barriers may exist in current laws protecting electronic communications or in antitrust law.

Organizations that share information may also be concerned that sharing or receiving such information may lead to increased civil liability, or that shared information may contain proprietary or confidential information that may be exposed to unauthorized use by competitors or government regulators.[82]

These legal implications have fueled debates among lawmakers and industry, suggesting that there is a great need for new laws to protect organizations from such liability. Proposed laws such as the Cyber Intelligence Sharing and Protection Act (CISPA) would allow for the sharing of Internet traffic information between the U.S. government and technology and manufacturing companies.[83] The bill would help the U.S. government investigate cyber threats and ensure the security of networks against cyberattacks. Unfortunately, new laws such as this have yet to be implemented because others disagree that enough privacy protection will be included in the laws.[84]

---

[80] Robinson and Disley, *Incentives and Challenges for Information Sharing*.

[81] Singer and Friedman, *Cybersecurity and Cyberwar*, 222–246.

[82] "ITI Recommendation: Addressing Liability Concerns Impeding More Effective Cybersecurity Information Sharing," Information Technology Industry Council, accessed September 2, 2014, http://www.itic.org/dotAsset/fae2feab-7b0e-45f4-9e74-64e4c9ece132.pdf.

[83] HR 624 Cyber Intelligence Sharing and Protection Act, (2013).

[84] Ibid.

In addition to legal barriers, this thesis will review policy barriers to cyber information-sharing. The debate includes organizational and national policies about what can be shared. Policies must exist within organizations to be able to share their data with other organizations. In reviewing the literature associated with cyber information-sharing and policy development, there are multiple areas where sources have identified a requirement for Congress to develop new policies for sharing cyber-threat information. Sharon Dawes proposes a theoretical model for understanding how policy, practice, and attitudes interact and suggests two policy principles, stewardship and usefulness, to promote the benefits and mitigate the risks of sharing.[85]

According to Dawes, successful sharing depends on a policy that takes a global view of how information resources can support government services. It should convey an affirmative expectation that government information be used to increase knowledge, improve analysis, and inform decisions as well as to administer programs. Any jurisdiction seeking the benefits of interagency information-sharing must adopt policies that do more than simply make sharing possible. It needs policies that make it probable that appropriate problems will be identified and that reasonable effort will lead to success. Dawes suggests two policy principles, information stewardship and information use.[86] These policy principles will be discussed later in this thesis.

The Mitre report includes trust-building policies as a way to building trust and has two components.[87] First, participants will develop trust in the cyber defense sharing network as participants feel that the information they contribute is protected. Second, the network provides them the opportunity to gather valuable information unavailable elsewhere, providing high value back to participants.

Technology for automated information-sharing is another barrier to sharing cyber information, but there are initiatives working to close the technology gap. In order to

85 Sharon S. Dawes, "Interagency Information Sharing: Expected Benefits, Manageable Risks," *Journal of Policy Analysis and Management* 15, no. 3 (1996): 377–394.

86 Ibid.

87 Vazquez et al., "Conceptual Framework for Cyber Defense Information Sharing," 1–17.

share information, there must be a common language and format of how and what to share. Standards on information security have been around for a long time. For example,

The standards that are needed for sharing cyber threat information are fairly new and not widely adopted yet. For example, there are the NIST SP-800 standards for security information systems. There are also the ISO/IEC 27000 series of standards that are part of a growing family of ISO/IEC Information Security Management Systems (ISMS) standards.[88] Several emerging cyber security standards show early promise. Two of them, the Structured Threat Indicator Exchange (STIX) and Incident Object Description Exchange Format (IODEF) could potentially play a pivotal role in protecting threat-related communication between sharing partners. Furthermore, there are overlapping standards that are causing problems for some agencies. For instance, five years ago, there were no known cyber structured standards available to exchange cyber threat information, but there are now overlapping cyber-sharing standards that compete for use within organizations.[89] According to Kathleen Moriarty of EMC Corporation, threat information-sharing efforts must affect the most efficient response, and in doing so, it must ensure the threats shared are actionable. She goes on to mention that there needs to be an efficient automated sharing model developed.[90] She argues that if multiple overlapping standards are developed, the automation of cyber threat information becomes a barrier to successful sharing. This thesis builds upon her work and attempts to identify ways to unify standards development in order to have a more consistent approach for cyber standards.

Other barriers to cyber information-sharing have been identified such as personnel clearance levels and the need to access classified cyber information, concerns with the value of the data once it is shared, and fears that automated sharing could lead to the

88 Yves Barlette and Vladislav V. Fomin, "The Adoption of Information Security Management Standards," in *Information Resources Management: Concepts, Methodologies, Tools, and Applications* (Hershey, PA: IGI Global, 2010), 69

89 Kathleen Moriarty, *Transforming Expectations for Threat-Intelligence Sharing* (Hopkinton, MA: EMC, 2013).

90 Ibid.

release of too much information.[91] According to U.S. federal classification guidance policy, information shall not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the United States' national security, and if it pertains to things such as military plans, weapons systems or operations, foreign government information, intelligence activities and others.[92] Policies such as these prevent the sharing of cyber threat information.

According to a *Government Information Quarterly* report by Harold C. Relyea, the federal government has not established comprehensive policies to effectively integrate state and city governments into the information-sharing process. According to the report, the Government Accountability Office (GAO) identified several barriers to sharing threat information with state and city governments. For example, federal agencies say they could not provide states and cities with information due to concerns over state and local officials' ability to secure and protect classified information, the officials' lack of security clearances, and the lack of integrated databases. GAO indicated that these barriers could be overcome with proper training, new equipment, and adequate security clearances.[93]

C. SUMMARY

The literature on cybersecurity information-sharing indicates that there are significant barriers to cyber information-sharing and that organizations, both private and public, have obstacles to overcome to ensure successful sharing and prevention of future cyberattacks. These obstacles include trust, legal, and technological barriers. Other obstacles include problems with privacy and lack of incentives to share. This thesis will contribute to the existing research literature by providing a current account of the landscape of what are the barriers to cyber information-sharing between public and private entities.

---

91 Ponemon Institute, *Exchanging Cyber Threat Intelligence: There Has to Be a Better Way* (Traverse City, MI: Ponemon Institute, 2014).

92 "The President, EO 13526: Executive Order 13526: Classified National Security Information, Memorandum of December 29, 2009, Implementation of the Executive Order 'Classified National Security Information', Order of December 29, 2009, Original Classification Authority: United States," *The Federal Register,* accessed September 9, 2014, http://www.archives.gov/isoo/pdf/cnsi-eo.pdf .

93 Harold C. Relyea, "Homeland Security and Information Sharing: Federal Policy Considerations," *Government Information Quarterly* 21, no. 4 (2004): 420–438.

THIS PAGE INTENTIONALLY LEFT BLANK

III. METHOD

A. INTRODUCTION

Through the sharing of cybersecurity information, stakeholders are provided timely information on the most critical threats. They can use this important information to implement an effective solution that will reduce the risk to their mission-essential services and data.

This thesis asks the questions, what are the primary barriers to cyber information-sharing between government and private sector organizations? And, how can these barriers may be overcome? While some private and public sector organizations have begun to share cybersecurity information, there are still many barriers that are preventing the ability to share more.

A qualitative method of analysis through review of literature sources was used to identify the barriers to cybersecurity information-sharing with an emphasis on issued of trust, law, policy, and technology. The data were researched, coded, and categorized into major themes related to the research question through the use of a software product designed for qualitative analysis called NVivo.

B. LITERATURE SOURCES

Literature sources, such as government documents, books, and websites were used to perform this study. The primary source books were focused on cyber security, collaboration, and information sharing. Google Scholar, Dudley Knox Library, and the Homeland Security Digital Library were used to search for books and other materials on the subject. Other sources included the websites for Department of Homeland Security, White House, and Congressional hearing sources. There were many journal and trusted news related websites that were used as well. The data collected to perform this study spanned several years and was gather from books, journals, websites, Congressional hearings and news organizations. Some notable works that were included were P.W. Singer and Allan Friedman's *Cybersecurity and Cyberwar What Everyone Needs to*

Know and Paul Rosenzweig's *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World.*

C. INSTRUMENT

Computer Assisted Qualitative Data Analysis Software (CAQDAS) called NVivo from QSR Corporation was used in data analysis for this study. NVivo has been known to support data analysis because of the software's ability to make the analysis transparent to other researchers, its ability to manage large amounts of data, and its associated search and retrieval features. There are many benefits from using a product like NVivo such as creation of auditable footprints, allowing the research to be more explicit and reflective on the process, providing increased transparency, and providing new opportunities for data analysis.[94]

NVivo helps organize data for easy retrieval and analysis. It takes the place of the manual method of copying data, selecting sections of text, highlighting, and organizing into folders. NVivo software makes it possible to collect the data with common topics in nodes that contain pointers to various sections of several documents.[95]

In addition to the NVivo software, the NVivo Toolkit was used to assist with the qualitative analysis. The NVivo Toolkit was developed by Maureen O'Neill, researcher at the University of the Sunshine Coast, Queensland, Australia. Through the use of the NVivo Toolkit, O'Neill asserts that it is possible to constantly interrogate the data, moving from lower order to higher order themes, and providing a higher degree study through four stages as shown in Figure 1.[96]

While NVivo software helps with recording and analysis of the data, it is not designed to be a mechanism to automatically reach conclusions. Hence, it is still the researcher who uses the NVivo software to organize data, continuously looking for relationships with or contradictions to the data, shadowing the data in broad literature and

---

94 Maureen O'Neill, "NVivo Toolkit," QSR Corporation, accessed April 19, 2014, http://explore.qsrinternational.com/nvivo-toolkit.

95 Bengt Edhlund, *NVivo Essentials*, Raleigh, NC: Lulu.com, 2007.

96 Ibid.

research context, and formulating findings. The core of NVivo is that the researcher is the one who analyses data and not the software itself.[97]

Key to the qualitative analysis process is diminishing any doubt surrounding the reliability and validity of qualitatively produced findings, and formulating a serious method of data analysis.[98] Successful research using qualitative data relies on the rigor and thoroughness of the data analysis methods. The findings of this study are validated based on the vast data collection and qualitative analysis tool that was used for analyzing, coding, and presenting the theme of the data. By using a tool such as NVivo, themes were rendered automatically from the data of the sources. Through reflection of the themes and the data, it allowed for re-examination and confirmed certain aspects of this research.

The NVivo Toolkit describes the process of using the software in four steps as explained in the next section. Each step must be completed before entering the next step. This model of qualitative research is similar to the process that was designed by Rudolph Sinkovics and Eva Alfoldi.[99]

D. PROCEDURES

Successful research using qualitative data relies on the rigor and thoroughness of the data analysis methods and how qualitative data can be rigorously analyzed. The following procedures were used in conducting this study:

- **Descriptive**: Enter data sources in to NVivo
- **Topic**: Organize and code data
- **Analytic**: Analyze and query data
- **Conclusion**: Draw answers from data

The first step, descriptive, involves entering the project details into NVivo such as the project information, and sources. The sources identified in the "Literature Review"

97 O'Neill, "NVivo Toolkit."

98 Matthew B. Miles and A. Michael Huberman, *Qualitative Data Analysis: An Expanded Sourcebook* (Thousand Oaks, CA: SAGE, 1994).

99 Rudolf R. Sinkovics and Eva A. Alfoldi, "Facilitating the Interaction between Theory and Data in Qualitative Research using CAQDAS," in *Qualitative Organizational Research: Core Methods and Current Challenges*, eds. Gillian Symon and Catherine Cassell (London: SAGE, 2012), 21.

chapter include internal sources such as websites, pdf documents, and Microsoft Word documents from literature of on cybersecurity information-sharing. The external sources are the books and other items that were cited using the tool RefWorks. RefWorks data were imported into NVivo and notes were used to record thoughts and observations about the data.

The details of the data sources collected were entered into the research project into NVivo sources, which contained the sub-sections of internals, memos and externals.[100] Internals are primary research materials that are imported or created in NVivo that serve as the data sources as noted above. This includes any combination of documents, PDFs, audio, video, pictures or data sets. Memos allow for storing memos and other recordings about the study. Externals are proxies that represent research materials that cannot be imported in to NVivo, such as books or manuscripts.

The second step in the process includes abstracting obvious topics from the sources to create nodes. A node is basically a subject, concept, process, or idea. In this thesis, the nodes equate to the thesis research. The nodes that emerged as a result of this research include trust, legal, policy, and technology as the main barriers to cyber information-sharing.

The third step is to analyze the data in the sources and merge the nodes into sets or model the data into relationships by querying the data. This analytic step involved the initial merging of nodes and the running of queries. This helps narrow down the top barriers to cyber information-sharing. For example, the initial nodes for the legal node included many nodes such as privacy laws, antitrust laws, other cyber laws, and so on. After querying and researching more on the subject, the data emerged into a single node to be legal. Alan Bryman suggests that this is the process of exploring more complex aspects of the nodes.[101] This will be described in more detail in the next section.

---

100 Alan Bryman, *Social Research Methods* (Oxford: Oxford University Press, 2012).

The sources analyzed for this thesis included approximately 400 items, including available unclassified U.S. government reports and studies on cyber issues for the past decade as well as academic and other studies available through the NPS Dudley Knox Library and other locations.

101 Ibid.

The last step is to reach a conclusion. Conclusions are more readily verified as the analysis continues, but certainly do not completely appear until the data collection is finalized.[102] For this study, NVivo assisted in organizing the data so the analysis could draw conclusions that were reliable and unproblematic. Chapter V will cover the conclusions from this study.

E. DATA ANALYSIS

Thematic analysis was used to capture important categories in the data in relation to the research questions. It revealed patterns and made sense of the data in a meaningful way. The data served as evidence for the themes and relationships that were established.

Through the use of NVivo's automatic coding mechanisms, obvious topics were drawn from the sources and the data were coded. Coding in NVivo allows for the grouping of related concepts to be organized in containers, the aforementioned nodes. This process is facilitated by allocating coding stripes and highlighting certain phrases and sentences, which denotes obvious topics that had originated from the formulation of nodes. The following figure shows the nodes and coding stripes for this study that were automatically marked in this study by using the Auto Code feature of NVivo.

[102] Matthew B. Miles and A. Michael Huberman, *The Qualitative Researcher's Companion* (Thousand Oaks, CA: SAGE, 2002).

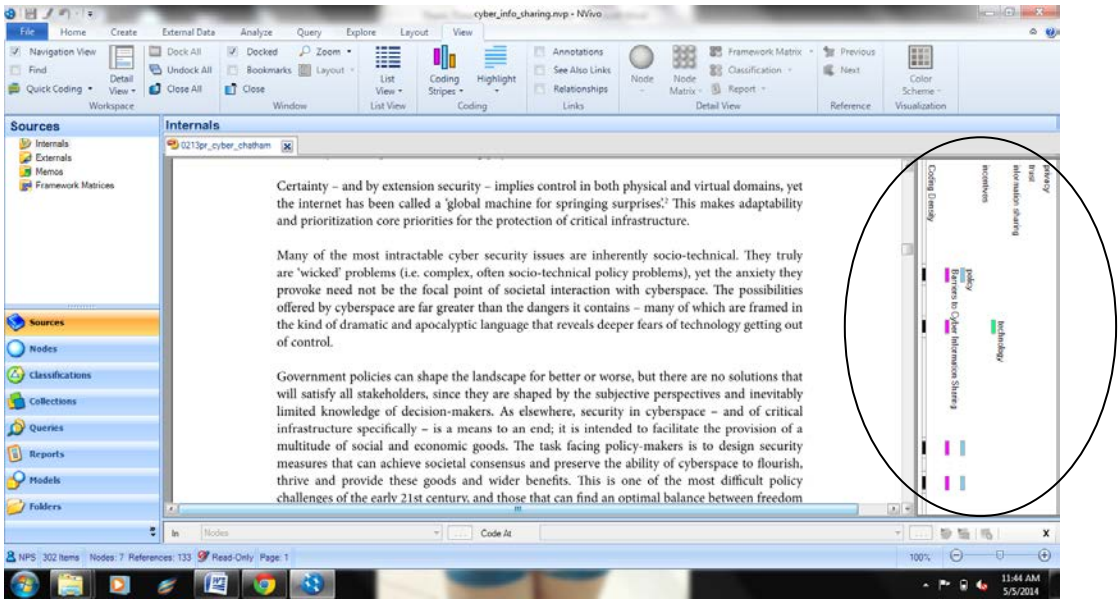

Figure 2. NVivo coding

Coding is the key process of analysis through NVivo. As nodes are described as the places to store ideas, coding is the way to store pointers to the text about those ideas. Coding is the computerized equivalent of putting all the relevant material into a file folder per each node. Coding not only allows users to find relevant data to research questions quickly, but it also helps to obtain and refine clues from materials. The coding in Figure 2 shows the relevant coverage of the barriers to cyber information-sharing and the coding stripes are shown in color at the right side.

The editing, coding, and analyzing process of NVivo could be endless because it can be used to continuously reorganize and refine research ideas. In brief, NVivo is used to help record and organize data, based on certain categories. NVivo's functions are used to assist with the analysis by making links, coding, sorting and doing simple statistics, thus finding out relationships or no relationships. It is more equivalent with this study's epistemology and methodology than free-mapping or pure quantitative studies.

By using the NVivo software tool, this thesis can help provide input for future research. The relevant theories of this work concerning information-sharing can further add to data analysis and discussion. For example, another researcher could show cyber analyst's influences toward sharing through the addition of standard operating procedures

and incident response data at a security operations center for further analysis. In this way, the relevant literature and analysis that was already performed can be utilized and reflected upon for continued research.

NVivo software is used to identify themes and classify the literature data. This is a very similar to that described for empirical data analysis. The analytic stage, step 3 of the NVivo Toolkit process, involved the initial merging of nodes and the running of queries. Bryman suggests that this is the process of exploring more complex aspects of the nodes.[103]

Earlier, the chapter touched on how the data are analyzed and refined through the use of queries. The example explained how the "legal" node emerged by running queries under the many different initial nodes for the different laws pertaining to cyber information-sharing such as privacy, intellectual property, liability, and antitrust law. By generating these queries, it was found to be much better to merge the nodes into the one node, legal.

Other queries that were performed were to find the legal barriers and why they were barriers. For example, the antitrust laws were found to be a barrier because of the query of the sources for antitrust. By having all the sources available to query, it was much easier to find the evidence needed to identify that antitrust was a major theme under the legal barriers to sharing. According to Amitai Aviram and Avishalom Tor, the contemporary assessment of the competitive effects of information-sharing among competitors is a showcase of the duality of public policy and antitrust law toward cooperation.[104] Scholars recognize the potential anti-competitive effects of information-sharing among competitors, but at the same time acknowledge the social benefits derived from this business practice.[105]

Through NVivo's coding process, queries, merging and continued analysis, the nodes that emerged to the top of the analysis were trust, technology, policy, and legal.

---

[103] Bryman, *Social Research Methods.*

[104] Avishalom Tor and Amitai Aviram, "Overcoming Impediments to Information Sharing." *Alabama Law Review* 55, no. 2 (Winter 2004): 231–279.

[105] Tor and Aviram, "Overcoming Impediments to Information Sharing."

Therefore, the thematic analysis of the sources validated the fact that those are the main barriers to cyber information-sharing and will be the findings discussed in future chapters.

NVivo has multiple visualization options, including modeling, to display qualitative analysis data. The models, are used to show the relationships between the various items and to demonstrate the theory, or how the data supports the hypothesis. Tables can be used to find out the existence or non-existence of similarities, differences and relationships. The model in Figure 3 shows the barriers to cyber information-sharing from the thematic analysis of the external data sources.

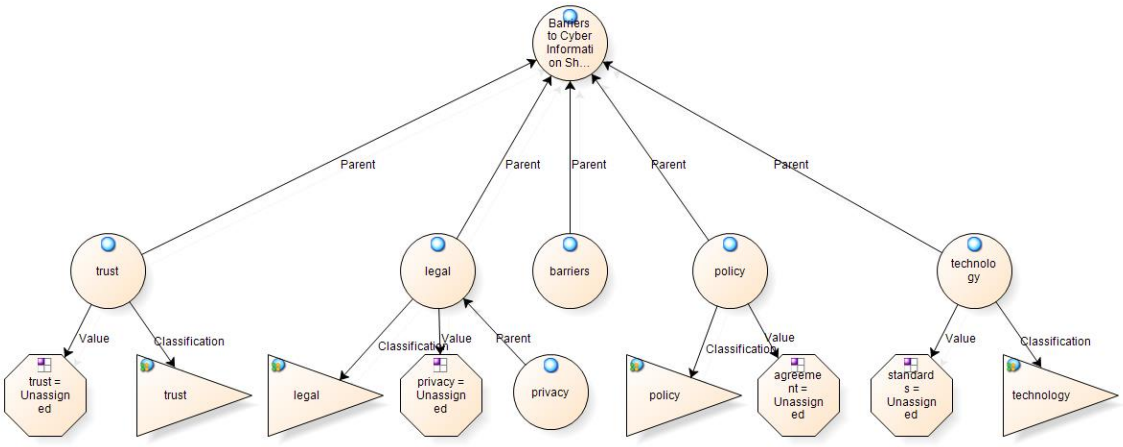

Figure 3. NVivo mapping model

It has been suggested that the qualitative researcher has few guidelines for reliable and thorough findings.[106] However, by using tools such as NVivo, a user is able to use techniques that ensure thoroughness and reliability in the analysis of the data with a higher degree of study and validation.

Conclusions are more readily verified as the analysis continues, but they do not completely appear until the data collection is finalized. For this study, NVivo assisted in organizing the data so the analysis could draw conclusions that were reliable and free from problems.

106 Miles and Huberman, *Qualitative Data Analysis*.

After completing the procedures in the four steps of the process, the author was able to translate from the NVivo project to consider the meaning of higher order themes for the discussion chapter. By using NVivo in support of this analysis, the major themes that emerged of the barriers to cybersecurity information-sharing include trust, legal, policy, and technology barriers. The conclusions were made by performing each of the four steps and enabled the development of the findings and recommendations of this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RESULTS

A. RESEARCH QUESTIONS

This study asks the questions, what are the primary barriers to cyber information-sharing between government and private sector organizations? And, how can these barriers can be overcome? While some private and public sector organizations have begun to share cybersecurity information, there are still many barriers that are preventing the ability to share more. As explained previously, more than 300 sources of information were gathered and researched (see Appendix A). Through the research of the literature and the use of NVivo to help organize and query the data, it is evident that the barriers to sharing cyber information are primarily trust, legal, policy, and technology. These major themes that emerged from the data provide a vivid observation of the barriers to cyber information-sharing. Figure 4 displays the results of the analysis and shows the total items that were coded and the number of coding references for each theme.

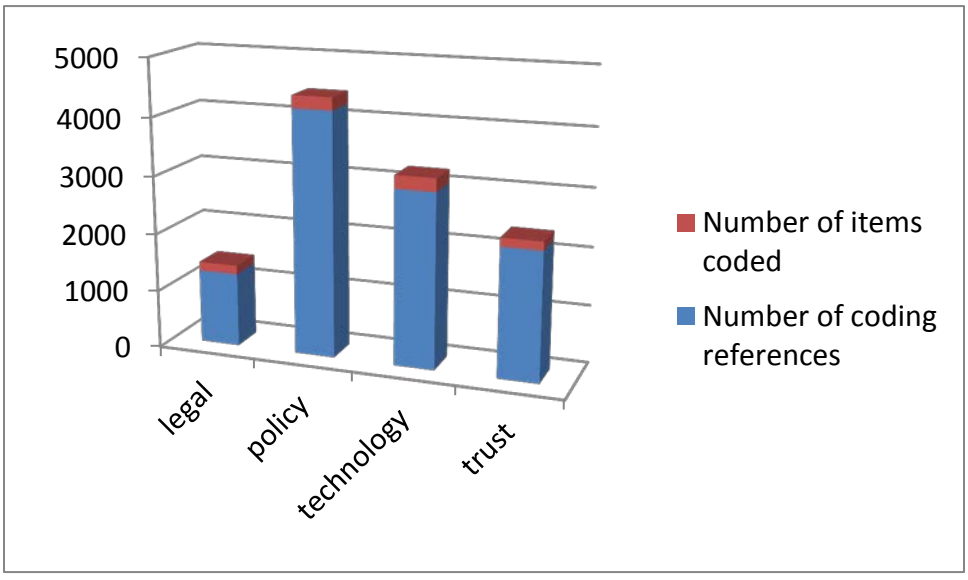

Figure 4. Results

1. Trust

The basic element of trust was identified as a major theme. There has been a lot of research and development in the field of computational trust in the past decade. Much of it has acknowledged or claimed that trust is a good thing.[107] Trust is an important factor when developing sharing partnerships and is found to be one of the major barriers to sharing cybersecurity information.

Trust is identified as one of the strategic keystones of the Office of the Director of National Intelligence (ODNI), Intelligence Community, Information Sharing Strategy.[108] According to the ODNI, the "need-to-know" culture led to practices that inhibit information-sharing today. Multiple organizations establish their own classification rules and procedures, resulting in inconsistent use and understanding of security markings. Differing requirements for access and certification and accreditation inhibit trust across the intelligence community. The key concepts are the need for consistent certification and accreditation practices, uniform information security standards, and uniformity across the intelligence community for accessing data to enable information-sharing.[109]

Additional evidence of the importance of trust is suggested by a study conducted by MITRE Corporation.[110] The study revealed a high degree of trust is required to share cybersecurity information and that is a barrier. In the study, MITRE found that it may be difficult to share cybersecurity-related information between a for-profit company and its competitors or among government agencies due to conflict-of-interest issues. The study also suggests that members may be reluctant to share information with another company that is trying to maximize profits while acting as a trusted third party.

In another study performed by the European Network and Information Security Agency (ENISA), it was noted that formal means for sharing information should be set

---

107 Stephen Marsh and Mark R. Dibben, "Trust, Untrust, Distrust and Mistrust–an Exploration of the Dark (Er) Side," in *Trust Management*, 17–33 (New York: Springer, 2005).

108 Office of the Director of National Intelligence, *United States Intelligence Community Information Sharing Strategy* (Washington, DC: Office of the Director of National Intelligence, Feb. 22, 2008).

109 Ibid.

110 "Cyber Information-Sharing Models: An Overview," Mitre, accessed February 12, 2014, http://www.mitre.org/sites/default/files/pdf/cyber_info_sharing.pdf.

up in order to improve the protection and rapid restoration of infrastructure critical to the reliability of communications within and throughout Europe.[111] The study finds that companies may be reluctant to share information directly with a government agency, due to fears of information being leaked or disclosed by Freedom of Information Act requests. In addition, there are cultural barriers that often lead companies to distrust the government. Companies need to feel that the benefits they gain by sharing sensitive information with the government must outweigh the risks; often, this barrier is not crossed.[112]

Other evidence that trust is a key factor for information-sharing is from a conference that was held in Boston, Massachusetts, at the Advanced Cyber Security Center (ACSC) in November 2013. The conference reviewed some of the barriers to cyber information-sharing and trust was a major topic. At the conference, Phyllis Schneck, deputy under secretary for cyber security for the National Protection and Programs Directorate of the U.S. Department of Homeland Security, stated that her number one priority is building trust between the government and the private sector. She also said that the cybersecurity community has the ability to defeat this adversary, by building trust. Furthermore, global situational awareness is the dream, and DHS plans to engaging people within the community to get their trust and by incentivizing companies.[113]

With the recent NSA leaks and the WikiLeaks problems there are even more trust barriers to cyber information-sharing between public and private entities.[114] In a recent *FedScoop* article, Dan Verton discusses the ongoing problem with the NSA Edward Snowden leaks and the problems faced with sharing cyber information with public and private sector because of the lack of trust based on leaked information.[115] According to the article, Larry Castro of the NSA said that the Snowden's unauthorized disclosures

---

111 Robinson and Disley, *Incentives and Challenges for Information Sharing*.

112 Ibid.

113 Blevins, "Experts Propose Better Cybersecurity Information-Sharing Models."

114 Ibid.

115 Dan Verton, "NSA Leaks Threaten Global Cybersecurity Information Sharing," *FedScoop*, October 16, 2013, http://fedscoop.com/nsa-leaks-threaten-global-cybersecurity-information-sharing/.

took the wind out of the sails of what was a growing agreement that the NSA had a very direct role to play in supporting the Department of Homeland Security (DHS) and providing actionable cyber-threat information.

The Office of the Director of National Intelligence (ODNI) was created based on the recommendation of the 9/11 Commission because of the failed intelligence sharing that could have prevented the attacks of that day.[116] After the WikiLeaks scandal, intelligence officials defended information-sharing practices, and claimed that it was possible to reconcile these practices with strong security.[117] They are likely about to come under renewed political pressure, as a result of Sunday's revelations. According to the *Washington Post*, after the leaked information, the ODNI and the Intelligence Community now have stricter rules for information.[118] Now that the leaked NSA information is in the open source, there are many implications that will plague us for this for years to come. Some experts agree that the leaks will make the United States require more transparency of federal programs.[119]

According to Col. Cedric Leighton, the former NSA deputy director of training at the Bloomberg Enterprise Technology Summit in New York City, , Snowden's leaks had performed a significant disservice to the worldwide health of the Internet.[120] Leighton was talking about the recent moves by Brazil and other countries to reconsider the decentralized nature of the foundation of the Internet.

Trust is a major theme in any type of information-sharing, not just cybersecurity. David Sutton, an expert in cybersecurity and critical infrastructure protection explains that whatever their focus, partnerships require that a fundamental level of trust be

---

116 National Commission on Terrorist Attacks upon the United States, *The 911 Commission Report*, 567.

117 *Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration: Hearing Before the Committee On Homeland Security and Governmental Affair*, 112th Cong (2011).

118 Henry Farrell, "Snowden-Type Leaks Will Force the U.S. to be More Transparent," *Washington Post Blog*, http://www.washingtonpost.com/blogs/monkey-cage/wp/2014/02/24/snowden-type-leaks-will-force-the-u-s-to-be-more-transparent/.

119 Ibid.

120 Zack Whittaker, "Former NSA Executive: Snowden Leaks Caused 'Significant Disservice' to the Internet," *ZDNet*, April 24, 2014, http://www.zdnet.com/former-nsa-deputy-director-snowden-leaks-caused-significant-disservice-to-the-Internet-7000028746/.

established between the partners in order to have any chance of success.[121] In parallel with trust, there is also a need to share information between partners, which must be carried out in a controlled and secure manner.[122] According to Sutton, the issue of trust is the fundamental to the formation of Public-Private Partnerships (PPPs). Furthermore, if trust cannot be established or if it breaks down for any reason, the extent to which information may be shared and the resulting effectiveness of a PPP will be significantly reduced.[123]

Issues related to trust need to be understood and addressed before an organization launches a new sharing initiative.[124] As this analysis shows, trust is the basic theme that is needed in order to be able to begin to share information. The next chapter will examine ways to overcome the trust issues such as using a trust relationship model approach to sharing as well as information-sharing agreements to legally bind the trust relationship.

2. Legal

Another theme that arose in the analysis as a main barrier to cyber information-sharing are legal issues. The findings revealed that the legal barriers to cybersecurity information-sharing are privacy, antitrust and liability issues, and protection of confidential information. According to the Heritage Foundation, the first element of any legislation must be to enable and foster information-sharing between the public and private sectors, and among private-sector.[125] Furthermore, any legislation must provide robust protection for privacy and individual freedoms.

The 112th Congress tried to pass comprehensive cybersecurity legislation. The Cyber Intelligence and Sharing Protection Act (CISPA), passed the House of

---

[121] Sutton, "The Issue of Trust and Information Sharing," 258–276.

[122] Ibid.

[123] Ibid.

[124] G. Scott Erickson and Helen N. Rothberg, "Knowledge Assets, E-Networks and Trust," in Jean-Marc Seigneur and Adam Slagell, eds., *Collaborative Computer Security and Trust Management* (Hershey, PA: Information Science Reference/IGI Global, 2010), 1.

[125] Steven Bucci, Paul Rosenzweig and David Inserra, *A Congressional Guide: Seven Steps to U.S. Security , Prosperity, and Freedom in Cyberspace* (Washington, DC: The Heritage Foundation, 2013).

Representatives, but no law was produced.[126] Also introduced was the Cybersecurity Act (CSA) of 2012, also known as the Lieberman–Collins bill. According to The Heritage Foundation, the CSA failed to pass because of differences among members of Congress regarding how the nation should approach the growing challenge of cybersecurity.[127] The key revision to the CSA made cybersecurity standards voluntary, but some agencies' regulations would have made them mandatory in specific sectors. Many stakeholders think that regulation is not the way to go for fostering sharing cybersecurity information; therefore, the CSA did not become law.[128]

The Cyberspace Policy Review explains that private organizations are concerned that certain federal laws might prevent full collaborative partnerships and operational information-sharing between the private sector and government.[129] An example of this cited in the review is collusion where information-sharing and collective planning occurs among members of the same sector under existing partnership. Another example is the reluctance to share because the company does not want to disclose sensitive or proprietary business information to federal government, such as vulnerabilities and data or network breaches.

Although there are laws to protect companies from this, such as the Trade Secrets Act and the Critical Infrastructure Information Act, which addresses concerns with respect to the Freedom of Information Act (FOIA), there is still much reluctance to share.[130] In addition, companies are also concerned about harm to their reputation, liability, or regulatory consequences in regards to sharing. This works both ways too, in that the federal government will limit the information it will share with the private

126 Cyber Intelligence Sharing and Protection Act, 2013. HR 624 (2013).

127 Bucci, Rosenzweig and Inserra, *A Congressional Guide*.

128 James L. Gattuso, *Ensuring Cybersecurity: More Red Tape is Not the Answer* (Washington, DC: The Heritage Foundation, June 5, 2012), http://www.heritage.org/research/reports/2012/06/cybersecurity-and-red-tape-more-regulations-not-the-answer.

129 The White House, *Cyberspace Policy Review*.

130 Uniform Trade Secrets Act with 1985 Amendments; Critical Infrastructure Information Act of 2002, Pub. L 107–296 (2002); Freedom of Information Act, (1967).

companies because of the need to protect sources and methods or the privacy rights of individuals.

Antitrust laws provide important safeguards against unfair competition, and FOIA helps ensure transparency in government that is essential to maintain public confidence. The civil liberties and privacy community has expressed concern that extending protections would only serve as a legal shield against liability.[131] In addition, the challenges of information-sharing can be further complicated by the global nature of the information and communications marketplace. When members of industry operating in the United States are foreign-owned, mandatory information-sharing, or exclusion of such companies from information-sharing regimes, can present trade implications.[132]

Sharing between the private sector and the government is challenging because of the legal protections that private sector needs in order to share their information. One problem is that private sector companies worry that information they share may be used against them by the government. In a report by the Congressional Research Service (CRS), policymakers argued that there is a need for the federal government and owners and operators of the nation's critical infrastructures to share information on vulnerabilities and threats and to promote information-sharing between the private and public sectors in order to protect critical assets from cybersecurity threats.[133] Private sector entities may wish to share information with one another about threats they have faced or are currently facing. They may also wish to collaborate on solutions to these issues. Additionally, the government may have information about cybersecurity threats that would be similarly useful to potential targets in the private sector. The government may see value in having access to information from the private sector about cybersecurity threats. The CRS report explains that obstacles to information-sharing may exist in current antitrust laws. Private entities that share information may be concerned that sharing cyber threat information may lead to increased civil liability, or that shared

131 The White House, *Cyberspace Policy Review*.

132 Ibid.

133 Edward C. Liu et al., *Cybersecurity: Selected Legal Issues* (CRS Report No. R42409) (Washington, DC: Congressional Research Service, 2012).

information may contain proprietary or confidential business information that may be used by competitors.

The Comprehensive National Cybersecurity Initiative #5 (CNCI-5) information-sharing architecture (ISA) provides the architecture guidance that the federal cyber centers use to enable cyber information-sharing. The ISA provides a risk chart and there are several a high risk items. One high risk item is that authorities and legal restrictions (or lack of clear guidance) may prevent sharing. The CNCI-5 program management team is working to resolve these risks through policy working groups that include legal representation from the centers.

In another report developed by analysts at U.S. STRATCOM, legal issues that specifically deal with cybersecurity and information-sharing are identified as the USA-PATRIOT Act (Patriot Act) Foreign Intelligence Surveillance Act (FISA) Federal Acquisition Regulation (FAR) Intellectual Property Antitrust Law Title 10 & Title 50 Freedom of Information Act (FOIA) and Federal Advisory Committee Act (FACA).[134] This report provides a comprehensive overview of the laws pertaining to cybersecurity and collaboration between public and private organizations such as the USA-PATRIOT Act (Patriot Act), and the Foreign Intelligence Surveillance Act (FISA). The legal recommendations include proposed amendments to laws cited as perceived or actual barriers to collaboration, which include the Foreign Intelligence Surveillance Act (FISA), the Freedom of Information Act (FOIA), Antitrust Law, and the Federal Advisory Committee Act (FACA).[135]

These same legal concerns were addressed in a report that was published over fourteen years ago by the U.S. Air Force Institute for National Security Studies. The USAF report also cited two additional legal issues, concerns about the release of national

134 Frederick Bartell et al., *Collaborating with the Private Sector* (Fort Belvoir: Defense Technical Information Center, August 2009).

135 Ibid.

security material and barriers with the cooperation with law enforcement agencies which are still concerns today.[136]

3. Policy

Another barrier to cybersecurity information-sharing and a theme that evolved from the analysis is policy issues. The policy issues can be categorized into three areas and consist of policies related to legal issues to include liability and privacy, inter-organizational agreements for sharing and connection, and other policy issues including organizational and federal policies for sharing cybersecurity information. According to the Heritage Foundation, Congress should pursue a cybersecurity policy that avoids a cumbersome and expensive regulatory approach and enables information-sharing instead of regulating it.[137]

a. Liability and Privacy Policy Concerns

According to a report by CSIS, organizations follow the guidance derived from the Executive Order 12333 that implements the Privacy Act of 1974 or the Electronic Communications Privacy Act (ECPA).[138] These documents ensure that privacy rights of U.S. persons are protected. The problem with these policies is that they were not developed with the idea that we had to defend networks from malicious activity.

Members of Congress have been engaged in cyber legislative discussions within the past few years. Although they generally agree that comprehensive cyber reforms are necessary to protect both private and government information systems, there are serious disagreements over the details of the development and implementation of policy.[139] For example, congressional staff has been debating about the role of the federal government

---

136 Steven M. Rinaldi, *Sharing the Knowledge: Government-Private Sector Partnerships to Enhance Information Securit*y (Colorado Springs, CO: USAF Institute for National Security Studies, 2000).

137 Bucci, Rosenzweig and Inserra, *A Congressional Guide*.

138 Adriane Lapointe, *Oversight for Cybersecurity Activities: Why Intelligence Policies Won't Work, and What Kind of Approach Will* (Washington, DC: Center for Strategic and International Studies, n.d.) http://csis.org/files/publication/101202_Oversight_for_Cybersecurity_Activities.pdf.

139 Bucci, Rosenzweig and Inserra, *A Congressional Guide*.

and the responsibility and capabilities of DHS.[140] In addition, they also have been debating about the role of the private sector and how information-sharing between private sector and government would be done. There are also debates over what standards should be used for protecting critical infrastructure as well as how to best develop the future of our cyber-security workforce.

These debates are hampered by the limitations of Executive Orders. Under current law, including the Electronic Communications Privacy Act and antitrust laws, the companies that wish to share information with the government in order to help thwart cyberattacks may face civil and possibly criminal penalties.[141] These liabilities prevent the private sector from sharing with the federal government. The Cybersecurity Intelligence Sharing and Protection Act (CISPA) introduced in both the 112th and 113th congressional sessions attempted to address these liabilities but failed to be approved.[142] The findings conclude that the government needs more policies in place to protect information systems and infrastructure. Since the Edward Snowden leaks the public has concerns about their private information possibly being used by the government.[143] Since private industry has a responsibility to both its consumers and the government, a further debate needs to happen in order to balance the issue of sharing between private sector and government.

According to the NIST, a key challenge for privacy has been the difficulty in reaching consensus on definition and scope management, given its nature of being context-dependent and relatively subjective.[144] The Fair Information Practice Principles (FIPPs)—developed in the early stages of computerization and data aggregation to address the handling of individuals' personal information has become foundational in the

---

140 Ibid.

141 Rinaldi, *Sharing the Knowledge.*

142 Pauline C. Reich, "Culture Clashes: Freedom, Privacy, and Government Surveillance Issues Arising in Relation to National Security and Internet Use," in *Law, Policy, and Technology* (Hershey PA: IGI Global, 2012), 200–278.

143 Whittaker, "Former NSA Executive."

144 "NIST Roadmap for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology (NIST), February 12 2014, http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf.

current conception of privacy. They have been used as a basis for a number of laws and regulations, as well as various sets of privacy principles and frameworks around the world.[145] The FIPPs, however, are a process-oriented set of principles for handling personal information. They do not purport to define privacy in a way that has enabled the development of a risk management model nor do they provide specific technical standards or best practices that can guide organizations in implementing consistent processes to avoid violating the privacy of individuals.

Furthermore, the lack of risk management model, standards, and supporting privacy metrics, makes it difficult to assess the effectiveness of an organization's privacy protection methods. Policies are often designed to address business risks that arise out of privacy violations, such as reputation or liability risks, rather than focusing on minimizing the risk of harm at an individual or societal level. According to NIST, there are few identifiable technical standards or best practices to mitigate the impact of cybersecurity activities on individuals' privacy or civil liberties.[146]

b. Sharing and Interconnection Agreements

There is a lack of clearly defined steps that industry can take when partnering in government cybersecurity activities. Some recommendations identified in the literature were from Mitre and the Enduring Security Framework Operations Group. The recommendation was that the government should initiate government-industry agreements that enable industry to share information that is protected and aligned with other information that is provided by the industry.[147] This information can be used in a non-attributed type of product that can then be shared with other participants. The agreement needs to clearly define when and to what extent information is shared.

In addition, the agreement should include specific clauses that are common to all industry participants and that may be tailored to specific aspects of the sharing

145 "NIST Cybersecurity Framework," NIST, accessed June 2, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

146 Ibid.

147 Fernandez Vazquez et al., "Conceptual Framework for Cyber Defense Information Sharing within Trust Relationships."

transactions.[148] For example, the clauses may include specific information about an individual company's particular involvement, where the entire agreement outlines all expectations and limitations on overall industry involvement in the initiative. Furthermore, as new companies are incorporated into the sharing initiative, modifications for their particular agreement should be identified and included as best practices for other agreements that are under development.[149]

c. Federal Cyber Sharing Policies

According to the Federal Trade Commission (FTC) antitrust guidelines, sector specific agencies should coordinate with the Department of Justice (DOJ) Antitrust Division in the development of a critical infrastructure protection business review training module that will outline the process available to industry for collaborations with critical infrastructure protection partners.[150] In addition, the sector specific agencies in conjunction with the DOJ should provide training on the aspects of antitrust specifically related to cybersecurity efforts and antitrust compliance so that government and industry remain educated on and sensitive to methods that can mitigate this concern and ensure antitrust compliance.[151]

4. Technology

Technology issues, specifically the automation of cyber information-sharing, were also identified in the analysis as a barrier to cyber information-sharing. The cybersecurity information needed to be shared includes cyber threat indicators, malware findings, incidents, and victim information. Currently, these types of data are shared in the way of reports via email, websites, and data feeds. The reports are shared as word documents, PDF files, or even XML feeds via email or links from websites. There is very little in the

---

148 Enduring Security Framework Operations Group, *Threat and Vulnerability Information Sharing Working Panel Final Report* (unpublished manuscript, January 2010).

149 Ibid.

150 Federal Trade Commission (FTC) and the U.S. Department of Justice (DOJ), *Antitrust Guidelines for Collaborations among Competitors,* April 2000, http://www.ftc.gov/sites/default/files/documents /public_events/joint-venture-hearings-antitrust-guidelines-collaboration-among-competitors/ftcdojguidelines-2.pdf.

151 Ibid.

way of automated information-sharing. The automated sharing of cyber information is the main push for organizations and is identified as one of the main barriers.

Differences in technological capabilities of government agencies and in the private sector such as the availability of information-sharing capabilities and skilled employees to develop these systems present an important challenge in cyber information-sharing. Furthermore, the lack of standardized systems and data structures limit the success of information-sharing initiatives. The technologies needed to enable a successful cyber information-sharing capability should include middleware services such as web services and data transformation services, web portals, content management and content discovery, identity control and access management (ICAM) and data tagging, structured languages to share common data, and cross domain solutions to enable sharing across multiple security domains. The next chapter will provide a discussion of the technology recommendations for a successful information-sharing architecture.

B. VALIDITY OF FINDINGS

The validity of these results is addressed by constantly reviewing the findings and querying the data with multiple query terms. Any relevant new data that emerged from this step was integrated into the findings for further analysis. In addition, NVivo software was used to assist with organization of content, coding, and theme identification by providing the automated capability to narrow down the results of the thesis and therefore identifying the findings. According to Creswell, the advantages of using a computer program to assist with data analysis is that it provides a way to organize and file data for quick access; it forces the investigator to look closely at the data and think about what each sentence might mean; it provides a mapping feature which allows visibility into the relationships among the data; finally, it allows easy retrieval of the data.[152]

[152] John W. Creswell, *Qualitative Inquiry and Research Design: Choosing among Five Approaches* (Thousand Oaks, CA: SAGE, 2012).

THIS PAGE INTENTIONALLY LEFT BLANK

V. FINDINGS

A. INTRODUCTION

This thesis identified some of the primary barriers to cyber information-sharing between government and the private sector and how these barriers may be overcome. Through the study, it has been determined that if organizations implemented better practices of sharing cyber threat information, they could use this information to protect their networks and ultimately our infrastructure would be more secure.

After analyzing the data from the sources of this study, it is evident that the barriers to sharing of cybersecurity information are not much different than barriers when sharing other types of information such as law enforcement or intelligence information. The major factors that contribute to cyber information-sharing barriers were found to be trust, legal, policy, and technology. The next section will identify the factors to enable more successful sharing of cyber information such as incentives, trust relationships, and sharing agreements, better standards, and the NIST cyber framework,

According to Paul Rosenzweig and David Inserra of The Heritage Foundation, sharing cybersecurity intelligence information between the private and public sectors is important because it alerts companies and agencies to likely attacks or specific problems in the software.[153] In order for information-sharing efforts to be effective, the government should organize sharing efforts in order for this information to flow more rapidly, preferably in an automated fashion. When sharing cyber intelligence information, the private sector needs to be provided with legal, FOIA, and regulatory protections so they are not punished when they do share. Information sharing should be broad enough to ensure that government agencies have the actionable intelligence they need in order to prevent cybercrime and attacks. Finally, information-sharing must have robust, but not restrictive, oversight to ensure that information is used appropriately.

153 David Inserra and Paul Rosenzweig, *Cybersecurity Information Sharing: One Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace* (Washington, DC: Heritage Foundation, April 1, 2014).

B. OVERCOMING TRUST BARRIERS

According to Sutton, trust is something that develops over time.[154] The beginnings of a trusted relationship cannot easily be developed over long distances. It is through personal contact between private and public sector representatives over time when trust begins to develop. Furthermore, by sharing useful information between partners, trust is increased, and although a major incident is not a thing to be wished for, when one happens and the relationship works well together, the level of trust increases even further.

Another way in which trust may be developed is through regular emergency exercises. These can be based on scenarios likely to affect public and private sector alike, and can also act as a catalyst to find innovative ways of working together in a crisis.

In a recent survey done by the Ponemon Institute, the question was asked about what is the best way to exchange threat intelligence.[155] Many of the respondents suggested that a trusted intermediary that shares with other organizations was the best way to share. Another group of respondents suggested the use of a threat intelligence exchange service would be a good way to share cyber threat intelligence.

In an ENISA study of successful public private partnerships, one recommendation is about the importance of Trust Building Policies. The ENISA study reports that in information-sharing networks where information-sharing is the core service provided, a key requirement is a high degree of trust in the network itself (i.e., that the policies, membership rules, requirement for security clearance, and interaction type must have been carefully designed to support trust.[156]

Trust between entities need not be whole or persistent. Transient trust during a moment of crisis may allow for a piece of information to be shared between two entities that would have not otherwise been made available for consumption. A sliding trust scale

---

154 Sutton, "The Issue of Trust and Information Sharing," 258–276.

155 Ponemon Institute, E*xchanging Cyber Threat Intelligence*.

156 "Cooperative Models for Effective Public Private Partnerships," ENISA, accessed February 15, 2014, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps/copy_of_desktop-reserach-on-public-private-partnerships.

is influenced by operational need and quality of relationship. It must be incorporated into a sharing network for information-sharing relationships that change over time. In this case, the partner you don't trust today may be your best friend tomorrow.

Trust relationships must span the different engagement levels: from the organizational leadership that empower their staff to produce and consume information to the technical staff that ultimately will use the information. Having an institutional process for guiding these types of relationships is central to the success of an organization as a whole in participating in information-sharing networks. To support these processes, organizations will need to focus on the trust scale while leveraging mechanisms and tools to support the mapping and perception of these relationships.

Trust relationships are affected by both the organizational and ethnic cultures of the sharing entities. There are cultures where no information-sharing will take place until a maturity point is reached in the relationship. Then there are ethnic cultures where a business need will drive information-sharing even though the relationship has not matured enough for sustained information-sharing between entities.

According to the Information Sharing Strategy of the Intelligence Community, confidence in the information and confidence in the people who has access to the information are all essential elements trust. The role of information quality of an information-sharing exchange can help build trust and mitigate risk.[157] One way to do this is to include a system that integrates attribute-based access, automated user authorization and auditing, and security at the data-level to enable a trust-based model for the free-flow of information among participants.[158]

The findings of the Ponemon study concluded that trusted intermediaries involved in the sharing of threat intelligence would improve current approaches to sharing threat intelligence. The best two ways to exchange threat intelligence are with a trusted

---

157 Andreas I. Nicolaou and D. Harrison McKnight, "Perceived Information Quality in Data Exchanges: Effects on Risk, Trust, and Intention to Use," *Information Systems Research* 17, no. 4 (2006): 332–351.

158 Office of the Director of National Intelligence, *United States Intelligence Community Information Sharing Strategy*.

intermediary that shares with other organizations and with a threat intelligence exchange service. They found that it is not as popular to share directly with other organizations or with a government entity that share with other organizations.

C. THE LEGAL DEBATE

The findings revealed that the legal barriers to cybersecurity information-sharing are privacy, antitrust, liability, and protection of confidential information. The following discussion points focus around these findings.

1. Privacy

Cybersecurity information shared for collaborative purposes might be used by competitors for commercial purposes, including such cases when government is a customer of either the initial company or a competitor. Government should initiate government-industry agreements that enable industry to share information that is protected and aligned with other industry-provided information. This will be fused in a non-attributed product to be shared with other participants. The agreement incorporates specific clauses defining the protection of commercial opportunities.

In a research paper, Rachel Nyswander Thomas of the Center for Strategic and International Studies proposed legislation that would center public- and private-sector cybersecurity collaboration onto a single objective such as research and development.[159] She proposes "civic switchboards," a mechanism for connecting resources among organizations that requires little government control. Thomas says two civic switchboards would be necessary to improve national cybersecurity-—a government-controlled one for information-sharing and incident response, and a nonprofit one for other objectives, such as research and development, technical standard setting and building human capital. In some cases, the government civic switchboard would act as an intermediary between existing public-private partnerships and in others foster the creation of new ones, she says. Thomas cites the Obama administration's Startup American Partnership as an

[159] Rachel Nyswander Thomas, *Securing Cyberspace through Public-Private Partnership A Comparative Analysis of Partnership Models* (Washington, DC: Georgetown University, May 2012).

example of a civic switchboard-like entity; the partnership is a nonprofit convened at the behest of the Small Business Administration that seeks to promote entrepreneurship.

2. Antitrust

In a discussion paper by Avishalom Tor and Amitai Aviram titled "Overcoming Impediments to Information Sharing," an assessment of the competitive effects of information-sharing among competitors is provided along with an outcome for a framework for public policy and antitrust law towards cooperation.[160] Tor and Aviram claim that the behavioral approach to antitrust law draws on a large body of empirical behavioral evidence to inform antitrust doctrine and policymaking. In particular, behavioral antitrust focuses on findings that reveal how the judgment and decision behaviors of actual antitrust actors are likely to systematically and predictably deviate from the strict rationality that antitrust law currently assumes. Perhaps due to the dominance in antitrust of rationality-based law and economics—from the field's jurisprudence and enforcement policies to its legal and economic scholarship—behavioral findings took far longer to garner broad attention in antitrust law than in many other legal fields. In fact, until a few years ago, antitrust discourse largely neglected those behaviorally informed analyses offered by a small number of legal scholars.

One way to overcome the legal barriers is through education and clarity about the laws that are currently barriers such as anti-trust. In a recent document by the Federal Trade Commission (FTC) and the Department of Justice (DOJ), some private entities may be hesitant to share cyber threat information with each other because they have been told by their legal counsel that sharing of information among competitors may raise antitrust concerns.[161] FTC and DOJ do not believe that antitrust is a real barrier to cybersecurity information-sharing. According to the statement, while it is true that certain information-sharing agreements among competitors can raise competitive concerns, the sharing of the

---

160 Tor and Aviram, "Overcoming Impediments to Information Sharing," 231–279.

161 "FTC, DOJ Issue Antitrust Policy Statement on Sharing Cybersecurity Information," Federal Trade Commission, accessed May 18, 2014, http://www.ftc.gov/news-events/press-releases/2014/04/ftc-doj-issue-antitrust-policy-statement-sharing-cybersecurity.

cyber threat information is highly unlikely to lead to a reduction in competition and, consequently, would not be likely to raise antitrust concerns.[162]

According to the FTC and the DOJ, antitrust guidelines, business review letters, and advisory opinions explain the analytical framework for information-sharing and the competition issues that may arise with information exchanges generally.[163] The primary concern is that the sharing of competitively sensitive information—such as recent, current, and future prices, cost data, or output levels—may facilitate price or other competitive coordination among competitors. The joint DOJ/FTC *Antitrust Guidelines for Collaborations among Competitors* provide a good overview of how the Agencies analyze information-sharing as a general matter.[164]

According to the guidelines, Sector Specific Agencies should coordinate with the Department of Justice (DOJ) Antitrust Division and should provide annual training on aspects of antitrust specifically related to cybersecurity efforts and antitrust compliance so that government and industry may remain educated on and sensitive to methods that can mitigate this concern and ensure antitrust compliance.[165]

According to the White House, the announcement by the Department of Justice and the Federal Trade Commission that clarifies that cybersecurity information can be shared with competitors without violating antitrust law—long a perceived barrier to effective cybersecurity is important. These enforcing our antitrust laws, have made clear today that they do not believe "that antitrust is—or should b—a roadblock to legitimate cybersecurity information-sharing."[166]

3. Liability and Protection of Confidential Information

Private industry has reservations about sharing confidential or proprietary information with government about vulnerabilities or attacks because they worry that the

---

[162] Ibid.

[163] FTC and the DOJ, *Antitrust Guidelines.*

[164] Ibid

[165] Ibid.

[166] Daniel, "Getting Serious about Information Sharing for Cybersecurity."

information could be released to the public under the Freedom of Information Act (FOIA). FOIA permits the public, including industry, and the media, to request and receive information that has been shared within and to the government. Under current law that information would also be available through FOIA requests to foreign citizens and foreign governments. Industry has requested that an exemption to FOIA be provided for the sharing of "sensitive corporate security" information with government.[167] This is not a unique request and Congress has provided exemption in at least 60 different instances to prevent public disclosure of sensitive information.[168]

Providing trust and instilling confidence that the information shared will be protected is a significant and necessary step to ensuring that a two-way flow of information can occur resulting in improved infrastructure protection. Most organizations have existing processes in place to ensure the protection of privacy and civil liberties when it comes to sharing information outside of their organizations.

D. POLICY IMPLEMENTATIONS

1. Overcoming Liability Concerns

Future policies need to enable cyber information-sharing by removing ambiguities, providing strong protections to sharers, and establishing a public-private partnership to facilitate sharing. Entities that share cybersecurity information need certain protections.[169] These protections include exempting all shared information from FOIA requests and regulatory use, and providing information sharers with strong liability protection.

2. Information Sharing Agreements

Effective information-sharing requires the government to share fully and in a timely manner with the private sector through a public-private partnership established for this purpose. An Information Sharing Agreement (ISA) is an agreement made between

---

167 Freedom of Information Act, (1967).

168 Rak, *Information Sharing in the Cyber* Age, 50

169 Bucci, Rosenzweig and Inserra, *A Congressional Guide*.

two or more collaborating organizations which describe verification and compliance methodologies, and define the type of information and scope of sharing, how the information will be used, what access control policies are being used, what legal or policy frameworks exist for compliance of the information such as retention.[170]

3. Federal Sharing Policies

Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, which was signed by President Obama in February 2013, has the most comprehensive policy for sharing cybersecurity information between private sector and government. It directs Federal agencies to use their existing authorities and increase cooperation with the private sector to provide better protection for the systems that are critical to our national and economic security.[171]

In addition, President Obama signed the Presidential Policy Directive (PPD)-21, *Critical Infrastructure Security and Resilience*. While the EO establishes a number of specific programs to improve cybersecurity, it does so under the overall policy framework set out by PPD-21, which explains the President's commitment to partner with owners and operators to secure our Nation's critical infrastructure against threats.

According to DHS, the EO, and PPD updates policy from a primary focus on protecting critical infrastructure against terrorism to protecting, securing, and making the nation's critical infrastructure more resilient to all hazards, including natural disasters, manmade threats, pandemics, and cyberattacks.[172] Furthermore, it directs the executive branch to strengthen our capability to understand and efficiently share information about how well critical infrastructure systems are functioning and the consequences of potential failures.

---

170 "Multinational Experiment 7 Outcome 3—Cyber Domain Objective 3.2 Information Sharing Framework 22 January 2013," NATO, accessed September 15, 2014, http://csrc.nist.gov/cyberframework/rfi_comments/dod_js_j7_part_2_022713.pdf.

171 "The President, EO 13526: Executive Order 13526."

172 Department of Homeland Security (DHS), *Executive Order 13636: Improving Critical Infrastructure Cybersecurity Department of Homeland Security Integrated Task Force Incentives Study Analytic Report* (Washington, DC: DHS, June 12, 2013). http://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf.

Under Executive Order 13636, NIST has produced the first version of a voluntary framework for reducing cybersecurity risk to critical infrastructure, which includes a methodology for protecting individuals' privacy and civil liberties during the conduct of cybersecurity activities. Released in February 2014, the Framework for Improving Critical Infrastructure Cybersecurity was developed by collaborating extensively with critical infrastructure owners and operators, industry leaders, government partners, and other stakeholders. The accompanying NIST *Roadmap for Improving Critical Infrastructure Cybersecurity* identified the need for more privacy technical standards to support the privacy methodology.

The Roadmap identifies key areas of development, alignment, and collaboration.[173] These key areas include authentication, automated indicator sharing, conformity assessment, cybersecurity workforce, data analytics, alignment with the Federal Information Security Management Act (FISMA), international impacts and alignment, supply chain risk management, and technical privacy standards. The automated sharing of indicator information can provide organizations with timely, actionable information that they can use to detect and respond to cybersecurity events as they are occurring. Sharing indicators based on information that is discovered prior to and during incident response activities enables other organizations to deploy measures to detect, mitigate, and possibly prevent attacks as they occur.[174]

To address the privacy policy gaps that were identified in the previous chapter, NIST has held a two-day workshop in April to work through technical standards gaps issues. The focus was to advance privacy engineering as a foundation for the identification of technical standards and best practices that could be developed to mitigate the impact of cybersecurity activities on individuals' privacy or civil liberties.[175] The objective is to provide a standards-based tool along with privacy engineering practices that will help to evaluate the privacy posture of existing systems, enable the creation of

173 "NIST Roadmap for Improving Critical Infrastructure Cybersecurity."

174 Ibid.

175 NIST, "Summary of the Privacy Engineering Workshop at the National Institute of Standards and Technology April 9–10, 2014," NIST, accessed August 2, 2014, http://www.nist.gov/cyberframework/upload/privacy-workshop-summary-052114.pdf.

new systems that mitigate the risk of privacy harm and address privacy risks in a measurable way within an organization's overall risk management process. NIST will engage a broad community of stakeholders to facilitate this work. The outcome of the workshop is a report that identifies challenges in privacy engineering, and proposes a framework for understanding privacy risk and a methodology for designing privacy-enabled systems that would support outcome-driven privacy design and engineering practices. More workshops will be held to continue this body of work.

E. TECHNOLOGY

1. Enabling Cybersecurity Information Sharing

There are many technologies needed to enable a successful cyber information-sharing capability. These technologies may include user-facing capabilities such as portals, content and document management, collaboration, and content discovery. Other technologies include infrastructure capabilities such as service oriented architecture integration services, identity control and access management (ICAM) and data tagging, structured languages to provide common formats and support automated data exchange, and cross domain solutions to enable sharing across multiple security domains.

The Homeland Security Information Network (HSIN) is an example of a successful implementation of an information-sharing architecture. HSIN is the trusted network for homeland security mission operations to share Sensitive but unclassified (SBU) information. Federal, state, local, tribal, territorial, international and private sector homeland security partners use HSIN to manage operations, analyze data, send alerts and notices, and in general, share the information they need to do their jobs.[176]

The National Cyber Protection System Information Sharing (NCPS-IS) is the platform being developed by DHS for cybersecurity related information-sharing for

176 "Homeland Security Information Network–Intelligence," Department of Homeland Security, accessed August 21, 2014, http://www.dhs.gov/hsin-intelligence (accessed August 21, 2014).

public and private organizations.[177] The National Cybersecurity Protection System (NCPS) Program is an integrated system of Intrusion Detection, Intrusion Prevention, analytical, and information-sharing capabilities used to defend the Federal Government's information technology infrastructure from cyber threats.[178] NCPS-IS will help prevent cyber incidents from occurring through improved discovery of, dissemination of, and access to threat, vulnerability, and mitigation information. It will help reduce the time to respond to incidents through improved collaboration and coordination. Further, it will provide auditing of the information that is shared to ensure quality control and foster increased information-sharing through increased transparency and privacy assurance. The end result of increased sharing through the NCPS-IS will be an increase in the understanding of the entire threat to U.S. network systems and a cohesive and comprehensive defensive stance against network attacks.

2. Data Quality and Actionable Intelligence

Information quality is the degree to which information meets the needs of its users. Sometimes information which is high quality for one user is low quality for another. Further, the data that is shared must be actionable. In an October 2013 report on Threat Intelligence, Gartner essentially points out that most vendors are offering Cyber Threat information–not cyber threat intelligence and that "only a comparative few (vendors)…provide true intelligence capabilities."[179] Gartner defines cyber threat intelligence as "Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."

---

177 "Einstein 3 Accelerated Privacy Impact Assessment," Department of Homeland Security, accessed September 15, 2014, http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/PIA%20NPPD%20E3A%2020130419%20FINAL%20signed.pdf.

178 Department of Homeland Security, National Cybersecurity Protection System (NCPS) Information Sharing Concept of Operations. Washington, DC: DHS.

179 iSight Partners, *What is Cyber Threat Intelligence and Why Do I Need It?* Dallas: iSIGHT Partners Inc., 2014).

Cyber threat intelligence needs to include much more than raw data. It requires rich contextual information that can only be created with the application of human analysis. This contextual information includes an understanding of the past, present and future tactics, techniques and procedures (TTPs) of a wide variety of adversaries. It must also include the linkage between the technical indicators (e.g., IP addresses and domains associated with threats or hashes that "fingerprint" malicious files), adversaries, their motivations and intents, and information about who is being targeted. It also involves the identification and ongoing monitoring of threat actors and integration with analysts to develop the finished intelligence.

Organizations need to merge intelligence that is gathered through human analysis with technical intelligence. This will provide the rich, accurate and actionable intelligence that can inform decision makers. The technical intelligence can include such things as open-source data, indicators scraped from the underground and analysis of various malware toolkits, system log data, and information shared from industry groups or other sharing partners.

3. Cyber Standards

For cybersecurity information to be of high quality for an organization to take action on it, the information must be accessible, complete, accurate, relevant, coherent and valid. Furthermore, it must be in a format that can be understood by a person or be machine readable by a system. In order to address the machine readable format, the recent development of cyber threat sharing standards such as Structured Threat Information eXpression (STIX) and Incident Object Definition (IODEF) as well as Mandiant's OpenIOC (Indicators of Compromise) will enable application developers to utilize these standards to enable sharing.

According to Verizon, one must rely on evidence as for any investigation.[180] Some of the most important evidence is through gathering indicators of compromise (IOCs). IOC's are identifiable events and artifacts that suggest a security incident occurred. Consistently collecting and maintaining the right data sources provides an

[180] Verizon, *2013 Verizon Data Breach Investigation Report* (New York: Verizon, 2013).

organization with a resource from which to mine for IOCs, and a basic foundation for a stronger investigation.

The problem with these standards is that there may be political barriers to which are the best standards to be using for information-sharing. CNCI-5 has provided the funding for the development of Mitre's Structured Threat Information eXpression (STIX) and is the main format of how the cyber operation centers are sharing information. The problem with the use of STIX as the standard to use for sharing cyber threat information is that if other organizations-for example international centers-want to share with federal centers and they do not use STIX, it will be hard to share.

F. THE ROLE OF THE INFORMATION SHARING AND ANALYSIS CENTERS

In 1996, the Clinton administration created the President's Commission on Critical Infrastructure Protection (PCCIP) to study the U.S. critical infrastructures, determine vulnerabilities and propose a strategy to protect the nation.[181] A key finding of the PCCIP in its 1997 report examining the vulnerabilities in the critical infrastructures is the need for information-sharing through a public-private partnership to better prepare to combat cyber threats. Building on the recommendations of the PCCIP, the Clinton Administration issued Presidential Decision Directive 63 (PDD 63) in May 1998 as the centerpiece of the Administration's policy on Critical Infrastructure Protection. This policy defined the United States critical infrastructure, as 'those physical and cyber-based systems essential to the minimum operations of the economy and government. PDD 63 further defined these systems into six initial areas; telecommunications, energy, banking and finance, transportation, water systems and emergency services, both government and private. PDD 63 recognized the important role of the private sector as the owners and operators of nearly all elements of the critical infrastructure in protecting the nation's cyber well-being set to developing partnerships with industry to improve information-sharing on vulnerabilities in networked systems, best practices and incidents as a means to reduce the potential threats that existed at that time. To facilitate this information-

181 Rak, *Information Sharing in the Cyber Age*, 50.

sharing, PDD 63 charged the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism to encourage the creation of private-sector Information Sharing and Analysis Centers (ISACs) comprised of the sectors of the critical infrastructure. Federal Agencies were designated as Sector Liaisons with related industry ISACs to assist with problems related to their sector. The ISACs enable industry within a specific sector to share information on threats, vulnerabilities, and information about an attack. This allows the flow of information between the public and private sector on threats and vulnerabilities, therefore accelerating response. PDD-63 was updated in 2003 with Homeland Security Presidential Directive/HSPD-7 to reaffirm the partnership mission better protecting our critical infrastructures and to help minimize vulnerabilities; the DHS established ISAC's to allow critical sectors to share information and work together to help better protect the economy.

Today there are 18 ISACs for critical infrastructure. Of all of the ISACs, one stands out among the rest when it comes to a successful approach to cyber information-sharing. That ISAC is the Financial Services Information Sharing and Analysis Center (FS-ISAC). The FS-ISAC was established by the financial services sector in response to 1998's PDD-63 and co-ordinates security collaboration among banks.[182] The FS-ISAC is a not-for-profit organization formed to serve the needs of the financial services industry for the dissemination of physical and cybersecurity, threat, vulnerability, incident, and solution information. Later, Homeland Security Presidential Directive-7 updated the directive.[183] The update mandates that the public and private sectors share information about physical and cybersecurity threats and vulnerabilities to help protect U.S. critical infrastructure.

Another ISAC that is emerging as a leader in cyber information-sharing is the COMMs ISAC. The COMMs ISAC's mission is to facilitate voluntary collaboration and information-sharing among Government and industry in support of Executive Order

182 Antone Gonsalves, "How Retailers can Boost Security through Information Sharing," *CXO Media*, accessed August 21, 2014, http://www.csoonline.com/article/2156060/data-protection/how-retailers-can-boost-security-through-information-sharing.html.

183 Lech Janczewski and Andrew M. Colarik, *Cyber Warfare and Cyber Terrorism* (Hershey, PA: IGI Global, 2008).

12472 and the national critical infrastructure protection goals of Presidential Decision Directive 63 (PDD-63); to gather information on vulnerabilities, threats, intrusions, and anomalies from multiple sources; and to perform analysis with the goal of averting or mitigating impact on the telecommunications infrastructure.[184]

G. NIST CYBER FRAMEWORK AS A WAY FORWARD

Since Executive Order 13636 was issued, NIST has played a convening role in developing the Framework, drawing heavily on standards, guidelines, and best practices already available to address key cybersecurity needs. NIST also relied on organizations and individuals with experience in reducing cybersecurity risk and managing critical infrastructure. Organizations that are part of the critical infrastructure can use the Framework to better manage and reduce its cybersecurity risks.

Not all critical infrastructure organizations have a mature program and the technical expertise in place to identify, assess, and reduce cybersecurity risk. Many have not had the resources to keep up with the latest cybersecurity advances and challenges as they balance risks to their organizations. NIST intends for the Framework to be a basic, flexible, and adaptable tool for managing and reducing cybersecurity risks. It is intended to be a living document and will continue to be updated and improved as industry provides feedback on implementation. As the Framework is put into practice, lessons learned will be integrated into future versions. This will ensure it is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions. NIST will also hold one or more workshops and focused meetings on specific areas for development, alignment, and collaboration.

The NIST Cybersecurity Framework is just a piece of the puzzle in the evolution of cybersecurity, one in which the balance is shifting to proactive risk-management standards. While the Framework is voluntary, organizations across industries may gain significant benefits by adopting the guidelines. According to Price Waterhouse Coopers, for most organizations, whether they are owners, operators, or suppliers for critical

184 "National Cyber Incident Response Plan," Department of Homeland Security, accessed September 15, 2014, http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf.

infrastructure, the NIST Cybersecurity Framework may be well worth adopting solely for its stated goal of improving risk-based security.[185] But it also can deliver ancillary benefits that include effective collaboration and communication of security posture with executives and industry organizations, as well as potential future improvements in legal exposure and even assistance with regulatory compliance.

A guiding principle of the Framework is collaboration to share information and improve cybersecurity practices and threat intelligence. A recent report by Price Waterhouse Coopers (PwC), shows that companies with highly effective security practices make it a point to collaborate with others to advance security and threat awareness. One of the most effective collaboration methods is participation in Information Sharing and Analysis Centers (ISACs), which have gained traction in security-forward industries like financial services. PwC recommends that organizations actively participate in ISACs appropriate to their industry.[186]

According to Deloitte, even though adoption of NIST's cybersecurity framework for critical infrastructure providers is currently voluntary, CIOs who opt to apply it to enterprise risk management practices may improve their ability to calibrate not just their organizations' cyber risk, but also business risk more broadly, while more efficiently allocating the information security budget.[187]

The Framework means little, if it doesn't get adopted by industry though. In a recent report from the Mercatus Center at George Mason University, the authors claim that the Cybersecurity Framework threatens to undermine this largely functioning system by imposing a brittle, technocratic standard that benefits specific interests and diminishes the incentives for cybersecurity innovation.188 Further, they argue that instead of a

---

185 PricewaterhouseCoopers, *Why You Should Adopt the NIST Cybersecurity Framework* (London: PricewaterhouseCoopers, May 2014) http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf.

186 Ibid.

187 Deloitte, "NIST Cyber Security Framework: 4 Steps for CIOs," *Wall Street Journal*, January 14, 2014, http://deloitte.wsj.com/cio/2014/01/14/nist-cyber-security-framework-4-steps-cios-can-take-now/.

188 Eli Dourado and Andrea Castillo, *Why the Cybersecurity Framework Will Make Us Less Secure* (Fairfax, VA: Mercatus Center at George Mason University, 2014).

government-driven, technocratic solution, cybersecurity insurance is an attractive solution to the problem of critical infrastructure protection. Insurance coverage can be flexible and tailored to specific needs and would incentivize firms to consistently improve their internal cybersecurity so as to keep premiums manageable. The problem they recognize is that the insurance market is still underdeveloped.

Critical Infrastructure owners and operators must weigh cybersecurity costs and benefits against other business and operational requirements, on the basis of their particular market environment, and within existing fiscal or operational regulatory boundaries.[189] To address the concerns of adoption, the DHS Integrated Task Force (ITF) performed a study to recommend a set of incentives designed to promote adoption of the Cybersecurity Framework, evaluate the benefits and relative effectiveness of each of the incentives in promoting adoption of the Framework, and to determine which of the incentives require legislation and which can be provided under existing laws.[190] There are 14 broad categories of incentives to include things such as expedited security clearance processes, grants insurance, and tax incentives. For Information Sharing, incentives were identified for ensuring that framework owners and operators are informed of relevant real-time cyber threat information. For liability considerations, reduced liability in exchange for improved cybersecurity or increased liability for the consequences of poor security were identified.

As the Framework is in the beginning stages for implementation and adoption, there is more work that needs to be done. Success of the Framework along with many of these incentives is dependent on compliance with the identified cybersecurity standards and practices and the adoption of new technologies, processes, and procedures. There is much more work that can be studied in this area.

189 "Cybersecurity Incentives Material," Department of Homeland Security, accessed August 21, 2014, http://www.amwa.net/galleries/default-file/CybersecurityIncentivesMaterial.pdf.

190 DHS, *Incentives Study Analytic Report*.

H. CONCLUSION

Three major conclusions can be made from this study. The first conclusion is that the exchange of cybersecurity information is critical in order to help organizations mitigate the security threats they face. With more and more sophisticated cyber criminals it is difficult, costly and ineffective to fight online attacks alone. Having the ability to connect and share information about existing and emerging threats could measurably improve an organization's cyber defenses.

Second, many organizations are either fully or partially participating in the exchange of cyber threat intelligence. However, there is much that needs to be done to improve collaboration and benefit from information that identifies patterns and trends that reveal ongoing attacks and future hazards. According to The White House, the goal is for the government to be a reliable information-sharing partner, but only one of many. Companies that are targeted by criminals and nation state actors should establish information-sharing channels with the National Cybersecurity & Communications Integration Center at the Department of Homeland Security, law enforcement agencies such as the FBI and Secret Service, and with other relevant agencies; however, they should also build information-sharing relationships with private sector partners and organizations.[191]

Finally, sharing should be voluntary, in order to encourage true cooperation. Voluntary sharing allows organizations with privacy concerns to avoid sharing their information, while still receiving the information they need from the government. Strong liability protection is critical for those companies who share information and must be provided if a company is going to share with the government. The information shared by the private sector must be exempt from Freedom of Information Act (FOIA) requests. If shared information is exempted from FOIA and regulatory use, a company can share important data without fear that its competitive advantages will be lost to other firms or used by regulators to impose more rules or costs.

191 Daniel, "Getting Serious about Information Sharing for Cybersecurity."

Lastly, the government must share information with the private sector much more than it currently does in order to build trust by the private sector. President Obama's executive order 13636 and the NIST Cybersecurity Framework is a step in the right direction, but more must be done. With the evolution of the technical standards such as STIX and TAXII, we must further the development efforts in the automation of cyber information-sharing in order to get actionable intelligence shared at net-speed. Finally, with the development of the DHS NCPS-IS, the nation's cyber enterprise posture will have increased situational awareness through the sharing of cyber status and cyber risk among public and private participants.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX. NVIVO SOURCE SUMMARY

The following report generated from the NVivo software tool provides a list of sources that were used as research material for this thesis:

Total Words in Source	Total Paragraphs in Source	Number of Nodes Coding Source	Coded Percentage of Source	Number of Text References
Document				
Internals\\02_Current Cyber Threats				
906	44	5	0.0255	19
Internals\\03_Directives				
1955	98	7	0.0554	65
Internals\\05_Over-Classification Intelligence and Information Sharing				
1059	59	5	0.0296	25
Internals\\06_Technologies and Standards used to Classify and Share				
167	12	4	0.0592	6
Internals\\better_cyber_info_sharing_model				
1034	25	5	0.0471	29
Internals\\Bloomberg response				
1075	20	3	0.0028	4
Internals\\Build International CapacityTransOrgCrime_TOC				
1005	20	3	0.0035	4
Internals\\China Security Memo				
2034	35	3	0.0022	8
Internals\\CNA				
2343	96	4	0.0323	34
Internals\\cnbc_on_ecs				
761	22	3	0.0111	5
Internals\\csis_comm_on_cyber				

517	8	3	0.0068	6

Internals\\cyb_attacks

377	15	4	0.0263	7

Internals\\Cybersecurity and International Relations-links

101	18	4	0.0351	8

Internals\\dhs_finds_ecs_slow

1093	40	8	0.0415	24

Internals\\From Dept of State

1204	82	5	0.0112	17

Internals\\From the White House International strategy for Cyberspace

1364	25	4	0.0057	11

Internals\\from_mne7

1513	160	10	0.0613	75

Internals\\FY14+ Information Sharing Agreement_21Apr2014_Predecisional_to PWG-mp

1928	124	5	0.8117	70

Internals\\HISIN CONOPS draft 11_04

7133	354	6	0.0067	29

Internals\\ITF_Issue Paper 1_EO-PPD 20130813_v1

3463	197	7	0.0124	38

Internals\\myths

814	3	1	0.2044	4

Internals\\NCCIC Critical Information Requirements (NCIR) v7 with Federal Memorandum

997	93	1	0.0078	3

Internals\\NCCIC Director Critical Information Requirements 22 Apr 2011

824	57	2	0.1485	7

Internals\\NCCIC-1013 Preparing an Incident Summary (ICS-CERT) WD v0.1

788	177	1	0.1152	4

Internals\\NCPS_IS_CONOPS_v0.4_DRAFT

17986	1536	9	0.0126	181

Internals\\PM-ISE_Annual_Report_Section_4

3708	117	8	0.0263	66

Internals\\Research Proposal

4632	200	4	0.0040	16

Internals\\RIT Announcement

1340	98	5	0.0117	25

Internals\\The Next Generation of Ecosystem-Wide Information Sharing - NPPD

827	43	3	0.0123	7

Internals\\The U.S. Government is currently pursuing all of the following

654	14	1	0.0043	1

Internals\\0213pr_cyber_chatham

20898	515	7	0.0021	133

Internals\\081208_securingcyberspace_44

468	745	2	0.0000	8

Internals\\08Jun_Paxton_cyber_covert_channel

27424	1068	8	0.0032	237

Internals\\09Mar_Dulin (1)

24525	578	4	0.0008	107

Internals\\10.1007_s10551-008-9853-6

12500	283	7	0.0030	121

Internals\\10.1023_A_1022959131133

8871	314	5	0.0002	9

Internals\\100820-TWP-america-top-secret1

14405	375	6	0.0011	36

Internals\\101007+-+2007+National+Strategy+for+Homeland+Security+-+070001135

22445	411	9	0.0016	86

Internals\\101007+-+2007+National+Strategy+for+Homeland+Security+-+Fact+Sheet+-+0700011351

1526	37	5	0.0023	12

Internals\\10Dec_Corzine

25013	869	8	0.0014	111

Internals\\11_4982

17899	666	6	0.0010	53

Internals\\12113_NCCIP_summary

374	12	3	0.0088	4

Internals\\12192013-rsa-crystal-ball

124	25	1	0.0421	1

Internals\\12192013-year-in-review

1068	134	4	0.0015	5

Internals\\12Mar_Mulligan

33668	1808	8	0.0052	371

Internals\\13_Hunker

8208	279	9	0.0043	124

Internals\\1301.6263v1

9567	210	6	0.0007	17

Internals\\13-019 US-CERT Year In Review CY2012

1572	65	3	0.0044	8

Internals\\140410ftcdojcyberthreatstmt

3252	57	9	0.3979	121

Internals\\2012infosharingstrategy

6861	173	9	0.0186	209

Internals\\2012sharingstrategy_1

6861	173	9	0.0186	209

Internals\\2013_ISE_Annual_Report_Final

81609	3047	9	0.0129	1315

Internals\\20131014110951E7486FA0E23D9F6B6CD8D7BA93441D2D-x

4079	96	9	0.0149	107

Internals\\264-01-001_DHS_Intelligence_Enterprise

4574	212	5	0.0046	53

Internals\\305027

3252	57	9	0.3979	121

Internals\\3789-reducing-risks-of-reporting-corruption

3416	100	7	0.0033	36

Internals\\6_5_Vazquez&et al_TrustRelationships

7315	169	7	0.0165	161

Internals\\60396rpt_cybercrime-cost_0713_ph4_0

9522	223	9	0.0081	133

Internals\\ADA435015

19127	517	12	0.0160	453

Internals\\ADA513209_Collab_with_private_sector

31295	753	12	0.0364	746

Internals\\ADA519879 (1)

8373	320	9	0.0214	162

Internals\\ADA587467 (1)

11605	523	5	0.0010	51

Internals\\aftergood_what_works_for_govt_secrecy

8741	341	10	0.0039	121

Internals\\analysis_senate_cyberbills_2012

6379	123	8	0.0117	79

Internals\\An-Approach-to-Unified-Trust-Management-Framework

11461	327	4	0.0195	1195

Internals\\Andersen-TTC_Cyber_Security_sp13

944	124	4	0.0086	22

Internals\\An-Overview-of-the-Community-Cyber-Security-Maturity-Model

6497	98	2	0.0237	18

Internals\\Arnwine-TTC_Cyber_Security_sp13

3062	455	2	0.0011	10

Internals\\BA13-051CybersecurityEOVP

4945	106	6	0.0051	39

Internals\\Balancing-the-Public-Policy-Drivers-in-the-Tension-between-Privacy-and-Security

11433	204	5	0.0123	272

Internals\\BILLS-113hr2281ih

3235	128	4	0.0047	20

Internals\\Blohm-TTC_Cyber_Security_sp13

2699	301	3	0.0015	11

Internals\\Bostrom-TTC_Cyber_Security_sp13

2074	250	3	0.0005	4

Internals\\Bowman-TTC_Cyber_Security_sp13

356	45	2	0.0187	20

Internals\\BuildingTrust

6332	321	6	0.0016	39

Internals\\Card Breaches Catalyst for More Info Sharing

720	24	2	0.0277	2

Internals\\Challenges-in-Sharing-Computer-and-Network-Logs

8692	205	3	0.0013	25

Internals\\Chenok-TTC_Cyber_Security_sp13

541	39	3	0.0126	16

Internals\\CHRG-108hhrg88194

28699	504	2	0.0000	2

Internals\\CHRG-108hhrg98291

24300	396	9	0.0020	93

Internals\\CHRG-113hhrg85613

22487	347	5	0.0009	41
Internals\\CHS SLFC Report 2013 FINAL				
40824	924	8	0.0052	256
Internals\\CISO-RPT-0112				
14306	741	8	0.0046	104
Internals\\cispa_act				
12904	301	10	0.0044	74
Internals\\cnci				
2658	36	5	0.0062	37
Internals\\cnci_rollins_crs				
10136	220	6	0.0015	62
Internals\\CNCI-5 ISA Technical Implementation Plan v1 0				
15744	919	7	0.2766	311
Internals\\cnsi-clintoneo12958				
10198	243	4	0.0007	25
Internals\\Collaboration-and-E-Government				
7286	260	2	0.0003	12
Internals\\Collaborative Computer Security and Trust Management _ IGI Global				
1139	64	5	0.0081	48
Internals\\collusion_incentives				
6251	231	6	0.0044	26
Internals\\commission_report_on_reducing_secrecy				
124100	2796	9	0.0013	592
Internals\\Congress revives cyber legislation _ Federal Times _ federaltimes				
453	12	5	0.1026	10
Internals\\Council of Europe - OAS Ottawa				
880	72	4	0.0034	15

Internals\\Critical Infrastructures-Background, Policy, and Implementation_2011

19437	487	9	0.0037	217

Internals\\CRPT-113hrpt41

2316	98	3	0.0167	7

Internals\\CRS_Cybersecurity - Authoritative Reports and Resources v2

36779	2415	11	0.0059	583

Internals\\CSIAC_V2N1_WEB

21965	732	5	0.0396	100

Internals\\Culture-Clashes--Freedom-Privacy-and-Government-Surveillance-Issues-Arising-in-Relation-to-National-Security-and-Internet-Use

44280	999	5	0.0038	316

Internals\\Cuviello-TTC_Cyber_Security_sp13

1837	213	4	0.0018	12

Internals\\cyb_auth_report

36779	2415	11	0.0059	583

Internals\\cyber_defense_playbook

993	32	2	0.0043	4

Internals\\cyber_info_sharing_paper

19127	517	12	0.0160	453

Internals\\cyber_norm_in_UN

26093	647	7	0.0022	201

Internals\\cyber_octopus_WS_3_alexander_CCC_global_frame

570	55	2	0.0006	2

Internals\\Cyber-057

2631	61	5	0.0055	32

Internals\\Cyber-067_Legal

23814	465	10	0.0073	351

Internals\\Cybercom EA Conf- RDML Lytle

1162	147	4	0.0022	7

Internals\\Cyber-Espionage-Brochure

6016	175	6	0.0094	101

Internals\\cybersecurity_cnci5

2658	36	5	0.0062	37

Internals\\Cybersecurity_Internet_governance

1601	43	6	0.0027	10

Internals\\Cybersecurity-May21-Final

3232	120	9	0.0085	45

Internals\\Cyberspace_Policy_Review_final

28760	860	11	0.0095	810

Internals\\d03564t

25627	647	10	0.0037	174

Internals\\DHS Safeguarding Classified SBU Updated February 2012

8663	316	6	0.0005	10

Internals\\DHS Understanding Derivative Classification Marking - July 2011

59443	2173	8	0.0005	102

Internals\\DHS_ECS_PIA

7738	267	6	0.0071	101

Internals\\dhs_fedscoop

770	40	8	0.0073	16

Internals\\dhs_ig_intl_cyber

8888	291	6	0.0056	83

Internals\\dhs_info_sharing_and_safeguarding_strategy

9093	346	8	0.0176	173

Internals\\dhs_information_sharing_strategy

2938	92	7	0.0506	156

Internals\\DHS_NPPD_JCSP_PIA

6050	231	7	0.0075	83

Internals\\DHS_OIG_Report_Reducing_Classified_info

10271	340	6	0.0007	25

Internals\\DHS_OIGr_11-117_Sep11

326	57	2	0.0011	2

Internals\\dni_Vision_2015

8788	224	7	0.0030	70

Internals\\DOD_Info_Sharing_strategy

6040	196	8	0.0391	291

Internals\\DOD-DIB-SCM

8568	507	4	0.0015	36

Internals\\doj_oig_report

26525	715	7	0.0010	66

Internals\\dumitras11wine

6841	163	6	0.0008	14

Internals\\EDA-DOC Analysis

1432	53	1	0.0446	6

Internals\\EINSTEIN3Accelerated _E3A__CONOPS

15304	553	7	0.0022	70

Internals\\Eisensmith-TTC_Cyber_Security_sp13

755	88	3	0.0015	4

Internals\\EMC-transf-expect-for-threat-intell-sharing

3383	90	4	0.0094	27

Internals\\eo_12829

2774	87	2	0.0008	10

Internals\\EO_13142

740	18	2	0.0006	2

Internals\\EO_13526

14526	449	5	0.0003	17

Internals\\eo13292

11136	356	4	0.0002	7

Internals\\eo13636

3470	68	6	0.0062	46

Internals\\EO-PPD Fact Sheet 12March13

332	12	5	0.0107	10

Internals\\EOPPDWG Adoption Recommendations

860	33	7	0.0063	10

Internals\\Executive Order CyberSecurity

3056	48	6	0.0071	48

Internals\\failingbydesign

4677	118	3	0.0006	6

Internals\\fbi_infoshare

3326	116	7	0.0442	215

Internals\\federaltimes_new_law_NCCIPAct

463	29	4	0.0045	5

Internals\\FIPS-PUB-199-final

3748	151	5	0.0044	51

Internals\\forthcoming-cybersecurity-fr

850	41	5	0.0211	34

Internals\\Free-Speech-Aboard-the-Leaky-Ship-of-State

20031	430	9	0.0015	120

Internals\\ftcdojguidelines

15040	410	10	0.1547	187

Internals\\gao_13_187

34849	977	9	0.0049	345

Internals\\GAO_Critical_Insfrastructure_Protection_DHS

15969	391	5	0.0019	42

Internals\\gao_cyber_roles_highlights

2014	32	3	0.0013	5

Internals\\gao_cyber_roles_report

34849	977	9	0.0049	345

Internals\\GAO_Cybersecurity-National Strategy, Roles, and Responsibilities_2013

34849	977	9	0.0049	345

Internals\\gao_memo

34849	977	9	0.0049	345

Internals\\GAO_report

17513	388	7	0.0112	362

Internals\\GAO_report (2)

18202	693	9	0.0044	277

Internals\\gao_rpt

34849	977	9	0.0049	345

Internals\\Giving a Voice to Open Source Stakeholders

13028	416	7	0.0037	68

Internals\\GPO-CDOC-105sdoc2-8

12748	293	6	0.0009	43

Internals\\guidance-for-ecpa-issue-5-9-2014

3136	61	6	0.0524	34

Internals\\hathaway-findings-chapter

7387	147	8	0.0046	68

Internals\\Henry-TTC_Cyber_Security_sp13

1422	170	2	0.0010	4

Internals\\HHRG-113-FA14-20130321-SD002

20427	288	7	0.0020	76

Internals\\HHRG-113-HM08-Wstate-CallahanM-20130425

4404	92	5	0.0244	194

Internals\\HHRG-113-HM08-Wstate-EdwardsC-20130516

2388	54	4	0.0042	12

Internals\\HomelandSecurityActof2002

88314	2356	11	0.0029	621

Internals\\HS_and_Info_sharing_Policy_considerations

9417	119	8	0.0136	123

Internals\\human_factors_and_trust

9600	224	7	0.1109	140

Internals\\ICCRTS07_Ruddy

17809	788	3	0.0008	75

Internals\\Improvinginformationsharingforcybersecurity_ITI

3470	66	7	0.1558	53

Internals\\in_trust_env_everyone_is_responsible

6657	141	7	0.1498	182

Internals\\incidentives_for_p2pnetworks

6407	148	2	0.0006	5

Internals\\info_sh_and_collab_policies

4343	90	7	0.0086	53

Internals\\info_sharing_in_cyber_age_a_keyto_CIKR

3688	94	5	0.0168	80

Internals\\Information Sharing_ A Turning Point

960	45	2	0.0313	22

Internals\\Information-Security-in-Government

9586	370	5	0.1316	124

Internals\\Information-Sharing--A-Study-of-Information-Attributes-and-their-Relative-Significance-During-Catastrophic-Events

11338	333	7	0.0054	71

Internals\\Information-Sharing--A-Study-of-Information-Attributes-and-their-Relative-Significance-During-Catastrophic-Events (2)

11338	333	7	0.0054	71

Internals\\Information-Sharing--A-Study-of-Information-Attributes-and-their-Relative-Significance-During-Catastrophic-Events (3)

11338	333	7	0.0054	71

Internals\\InformationsharingCyberBreakoutRecap

734	48	2	0.0015	6

Internals\\Information-Sharing-for-CIP--Between-Policy-Theory-and-Practice

15478	339	4	0.0005	25

Internals\\INSA - Critical Issues for Cyber Assurance Policy Reform - 26Mar2009

8867	267	9	0.0048	106

Internals\\INSA+Cyber+Intelligence

8165	289	8	0.0033	59

Internals\\Integration-and-Information-Sharing-in-E-Government

2536	90	3	0.0005	6

Internals\\Intel_in_the_CW1

21700	448	5	0.0001	13

Internals\\intel_info

7917	160	6	0.0110	95

Internals\\international_strategy_for_cyberspace

10149	184	10	0.0053	151

Internals\\ISA_2_0_v0_2_Content_Draft2

22607	1428	6	0.3648	366

Internals\\ISA_2_0_v0_2_Content_Draft2 (2)

22607	1428	2	0.0000	8

Internals\\ispab_oct2012_lzelvin_nccic-overview

840	68	5	0.0062	13

Internals\\iss

7494	197	8	0.0358	285

Internals\\iss (2)

7494	197	8	0.0358	285

Internals\\ITUNationalCybersecurityStrategyGuide

34572	1251	10	0.0026	357

Internals\\Jones-TTC_Cyber_Security_sp13

1810	217	4	0.5000	8

Internals\\Knowledge-Assets-E-Networks-and-Trust

6260	138	3	0.0094	178

Internals\\kosar_doc

9490	294	6	0.0050	197

Internals\\Layered_Security_Architecture

1833	172	6	0.0042	38

Internals\\LEAP

13967	269	7	0.0055	72

Internals\\Leighton-TTC_Cyber_Security_sp13

458	55	4	0.0031	6

Internals\\Letter-TTC_Cyber_Security_sp13

794	82	3	0.0037	10

Internals\\LM-White-Paper-Intel-Driven-Defense

6429	178	5	0.0013	17

Internals\\Mandiant_APT1_Report

23799	974	6	0.0012	67

Internals\\markel_task_force

11115	345	8	0.0264	404

Internals\\McAfee_WhitePaper_Shady_RAT

3038	187	4	0.0034	23

Internals\\mgmt_role_in_cyber

9312	244	9	0.0791	124

Internals\\Microsoft_whitepaper

8238	267	6	0.0054	170

Internals\\mitre_ieee

4928	211	2	0.0003	4

Internals\\MNE7

11605	523	11	0.0125	258

Internals\\Muehleisen-TTC_Cyber_Security_sp13

1056	119	3	0.0010	4

Internals\\MuellerKuehnWEIS2013

11950	265	8	0.0054	165

Internals\\nat_strat_pub_diplomacy

9253	282	5	0.0012	38

Internals\\National_Strategy_for_Information_Sharing

15011	455	8	0.0130	234

Internals\\NationalCyberSecurityFrameworkManual

99749	3026	11	0.0031	1042

Internals\\NATO-Industry cooperation on cyber information sharing

2688	106	5	0.0089	30

Internals\\NCIRP_Interim_Version_September_2010

32854	996	8	0.0042	254

Internals\\NCPS E3A PIA

10767	329	6	0.0057	123

Internals\\ncrdic-cyber

2595	84	6	0.0047	30

Internals\\nctc_issues

5592	127	6	0.0025	20

Internals\\nifs

3315	93	3	0.0010	6

Internals\\nps11-033010-26

29999	715	9	0.0029	121

Internals\\nps16-040705-09

7116	218	3	0.0010	26

Internals\\nps26-070907-01

45862	1378	9	0.0042	257

Internals\\nps34-092607-01

8951	293	5	0.0025	47

Internals\\nps45-011210-06-history_Kosar

4117	127	4	0.0026	48

Internals\\nps49-072009-02

20975	576	8	0.0012	73

Internals\\nps49-083010-17_Sandia

12708	444	7	0.0016	38

Internals\\nps51-060311-03_rosenweig

4151	88	6	0.0023	30

Internals\\nps51-122110-11_kosar_doc

9490	294	6	0.0050	197

Internals\\nps52-010510-68_who_can_classify

571	24	3	0.0029	6

Internals\\nps56-072412-04_SecureIT

1570	64	7	0.0147	31

Internals\\nps58-032411-06

11005	306	7	0.0145	200

Internals\\nps59-032913-02

12925	286	10	0.0080	157

Internals\\nps60-041813-13

5881	379	3	0.0009	20

Internals\\nps62-042613-07

10767	378	6	0.0057	123

Internals\\nps62-051713-14HEARING

11671	148	6	0.0018	44

Internals\\nps66-022513-02

7738	267	6	0.0071	101

Internals\\NSA leaks threaten global cybersecurity information sharing - FedScoop

922	43	6	0.0412	43

Internals\\OIGr_11-117_Sep11

326	57	2	0.0011	2

Internals\\OIGr-11-117-Sep11

326	57	2	0.0011	2

Internals\\Orndorff-TTC_Cyber_Security_sp13

536	73	4	0.0066	6

Internals\\Orrin-TTC_Cyber_Security_sp13

1770	207	5	0.0124	105

Internals\\Overcoming Impediments to Information Sharing

26973	486	11	0.0183	508

Internals\\p85-moore

8809	230	5	0.0012	34

Internals\\Paradigm Change_Cybersecurity of Critical Infrastructure

24618	713	11	0.0050	383

Internals\\pentagon_trust_info_sharing

854	48	4	0.2077	17
Internals\\PLAW-111publ258				
2445	82	2	0.0029	6
Internals\\PLAW-111publ258_Reducing_Over_Classification				
2445	82	2	0.0029	6
Internals\\Ponemon Study				
6114	455	7	0.0023	38
Internals\\Presentation David Senty 2 december 2013				
934	105	6	0.0061	13
Internals\\Public-Private Information Sharing				
7059	222	10	0.0140	140
Internals\\Public-Private Information Sharing (1)				
7059	222	11	0.3441	211
Internals\\quist_compilations				
9899	284	4	0.0005	20
Internals\\quist_history_of_class_at_oakridge				
12373	481	3	0.0014	48
Internals\\R40427				
10136	220	6	0.0015	62
Internals\\R42114				
29609	1134	12	0.0071	384
Internals\\R42985				
39394	849	10	0.0035	506
Internals\\RAND_MG989				
32771	809	8	0.0007	69
Internals\\RAND_RR235				
27520	1443	7	0.0026	279

Internals\\Resetting the System

11553	428	9	0.0037	146

Internals\\retail_sharing

663	24	4	0.1078	12

Internals\\ridge_info_sharing

1174	61	3	0.0784	9

Internals\\RL33123_20070122

12672	463	6	0.0025	95

Internals\\Role-of-FS-ISAC-in-Countering-Cyber-Terrorism

3942	124	2	0.0001	4

Internals\\sans_standards

8134	280	4	0.0008	8

Internals\\sar_crs_rpt

11021	308	7	0.0145	200

Internals\\Scurlock-TTC_Cyber_Security_sp13

2612	270	6	0.0078	40

Internals\\Security industry in ‘rut,’ struggling to keep up with cybercriminals

719	29	3	0.0084	15

Internals\\Sharing Too Much Information_ - BankInfoSecurity

2748	67	5	0.0100	23

Internals\\Shrauder-TTC_Cyber_Security_sp13

1206	175	2	0.0012	4

Internals\\signed IA FY2011_FY2018 Strategic Plan

4665	190	6	0.0112	70

Internals\\slides-85-mile-3

1213	115	3	0.0038	17

Internals\\sox_study

32181	1694	6	0.0011	93

Internals\\SSRN-id2201033_eoppd_metrics

23670	676	10	0.0165	382

Internals\\stix-intro-handout

834	38	3	0.0035	4

Internals\\Strategic Intent for Information Sharing

1329	50	7	0.0374	54

Internals\\symantec_report

17318	897	6	0.0014	61

Internals\\Teamworking-for-Security--The-Collaborative-Approach

10792	290	4	0.0009	20

Internals\\Teicher-TTC_Cyber_Security_sp13

1608	320	2	0.0008	4

Internals\\Tensions-in-Collaborative-Cyber-Security-and-how-They-Affect-Incident-Detection-and-Response

16193	401	5	0.0027	112

Internals\\The-Adoption-of-Information-Security-Management-Standards--A-Literature-Review

10994	402	6	0.0818	134

Internals\\The-Issue-of-Trust-and-Information-Sharing-and-the-Question-of-Public-Private-Partnerships

9790	355	3	0.0031	155

Internals\\Toomer-TTC_Cyber_Security_sp13

1586	120	6	0.0099	33

Internals\\top secret america

5799	118	6	0.0007	9

Internals\\transforming-classification_PIDB

27365	672	9	0.0025	195

Internals\\trust

2648	81	5	0.0129	156

Internals\\trust_and_info_exchanges

14683	454	5	0.1400	321

Internals\\trust_untrust_distrust_mis

8396	174	6	0.3211	436

Internals\\Trust-Privacy-Tradeoffs-in-Distributed-Computing

4527	177	3	0.0194	298

Internals\\united_front

1319	55	3	0.2084	10

Internals\\us_cert_OIG

7599	260	6	0.0041	40

Internals\\Using-Annotations-for-Information-Sharing-in-a-Networked-Community

4301	126	4	0.0016	6

Internals\\Verizon Data Breach Investigation Report 2013

25755	1317	8	0.0006	37

Internals\\Visner-TTC_Cyber_Security_sp13

731	98	4	0.0033	6

Internals\\Watch SWO-ASWO Essential Tasks

3919	131	1	0.0029	8

Internals\\WH_article_on_info_sharing

995	36	7	0.1190	23

Internals\\Year_in_Review_FY2012_Final

2465	161	3	0.0008	3

LIST OF REFERENCES

Barlette, Yves, and Vladislav V. Fomin. "The Adoption of Information Security Management Standards," in *Information Resources Management: Concepts, Methodologies, Tools, and Applications*. Hershey, PA: IGI Global, 2010.

Bartell, Frederick, Carrie Lacy, Melissa Moraczewski, Tanya Nodlinski, Sarah Norris, Kate Prasse, Ashley Thomalla, and Katherine Zielinski. *Collaborating with the Private Sector*. Fort Belvoir: Defense Technical Information Center, August 2009.

Bartle, Caroline. "Spreading the Word: A Social-Psychological Exploration of Word-of-Mouth Traveler Information in the Digital Age." Master's thesis, University of the West of England, 2011. http://www2.uwe.ac.uk/faculties/FET/Research/cts/projects/reports/bartle_2011_thesis.pdf.

Bipartisan Policy Center Cybersecurity Task Force. *Public-Private Information Sharing*. Washington, DC: Bipartisan Policy Center, 2012. http://bipartisanpolicy.org/library/report/cybersecurity-task-force-public-private-information-sharing.

Blevins, Brandan. "Experts Propose Better Cybersecurity Information-Sharing Models." *TechTarget*, November 14, 2013. http://searchsecurity.techtarget.com/news/2240209036/Experts-propose-better-cybersecurity-information-sharing-models.

Bryman, Alan. *Social Research Methods*. Oxford: Oxford University Press, 2012.

Bucci, Steven, Paul Rosenzweig, and David Inserra. *A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace*. Washington, DC: The Heritage Foundation, 2013.

Bui, Yvonne N. *How to Write a Master's Thesis.* Thousand Oaks, CA: SAGE, 2013.

Bumiller, Elisabeth and Thom Shanker. "Panetta Warns of Dire Threat of Cyberattack on U.S." *New York Times,* October 11, 2012.

Clayton, Mark. "Alert: Major Cyber Attack Aimed at Natural Gas Pipeline Companies." *Christian Science Monitor*, May 5, 2012, http://www.csmonitor.com/USA/2012/0505/Alert-Major-cyber-attack-aimed-at-natural-gas-pipeline-companies.

Creswell, John W. *Qualitative Inquiry and Research Design: Choosing among Five Approaches.* Thousand Oaks, CA: SAGE, 2012.

Dawes, Sharon S. 1996. "Interagency Information Sharing: Expected Benefits, Manageable Risks." *Journal of Policy Analysis and Management* 15, no. 3 (1996): 377–394.

Deloitte. “NIST Cyber Security Framework: 4 Steps for CIOs.” *Wall Street Journal*, January 14, 2014. http://deloitte.wsj.com/cio/2014/01/14/nist-cyber-security-framework-4-steps-cios-can-take-now/.

Department of Homeland Security (DHS). “Cybersecurity Incentives Material.” Accessed August 21, 2014. http://www.amwa.net/galleries/default-file/CybersecurityIncentivesMaterial.pdf.

———. *Executive Order 13636: Improving Critical Infrastructure Cybersecurity Department of Homeland Security Integrated Task Force Incentives Study Analytic Repor*t. Washington, DC: DHS, June 12, 2013. http://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf.

———. “Fact Sheet: Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience.” March 2013. http://www.dhs.gov/publication/fact-sheet-eo-13636-improving-critical-infrastructure-cybersecurity-and-ppd-21-critical.

———. “Homeland Security Information Network–Intelligence.” Accessed August 21, 2014. http://www.dhs.gov/hsin-intelligence.

———. “National Cyber Incident Response Plan.” Accessed September 15, 2014. http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf.

Department of Homeland Security (DHS), National Cybersecurity and Communications Integration Center (NCCIC), United States Secret Service (USSS), Financial Sector Information Sharing and Analysis Center (FS-ISAC), and iSIGHT Partners. *POS Malware Technical Analysis: Indicators for Network Defenders* Washington, DC: Department of Homeland Security, January 16, 2014.

Dourado, Eli and Andrea Castillo. *Why the Cybersecurity Framework Will Make Us Less Secure*. Fairfax, VA: Mercatus Center at George Mason University, April 17, 2014.

Edhlund, Bengt. *NVivo Essentials*, Raleigh, NC: Lulu.com, 2007.

Enduring Security Framework Operations Group. “Threat and Vulnerability Information Sharing Working Panel Final Report.” Unpublished manuscript, 2010.

ENISA. “Cooperative Models for Effective Public Private Partnerships.” Accessed February 15, 2014. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps/copy_of_desktop-reserach-on-public-private-partnerships.

Erickson, G. Scott and Helen N. Rothberg. 2010. “Knowledge Assets, E-Networks and Trust.” In *Collaborative Computer Security and Trust Management*, edited by Jean-Marc Seigneur and Adam Slagell. Hershey, PA: Information Science Reference/IGI Global, 2010.

Farrell, Henry. “Snowden-Type Leaks Will Force the U.S. to Be More Transparent.” *Washington Post*, February 24, 2014. http://www.washingtonpost.com/blogs/monkey-cage/wp/2014/02/24/snowden-type-leaks-will-force-the-u-s-to-be-more-transparent/.

Federal Register, The. “The President, EO 13526: Executive Order 13526: Classified National Security Information, Memorandum of December 29, 2009, Implementation of the Executive Order ‘Classified National Security Information’, Order of December 29, 2009, Original Classification Authority: United States.” Accessed September 9, 2014. http://www.archives.gov/isoo/pdf/cnsi-eo.pdf.

Federal Trade Commission. “FTC, DOJ Issue Antitrust Policy Statement on Sharing Cybersecurity Information.” Accessed May 18, 2014. http://www.ftc.gov/news-events/press-releases/2014/04/ftc-doj-issue-antitrust-policy-statement-sharing-cybersecurity.

Fernandez Vazquez, D., O. Pastor Acosta, Sarah Brown, Emily Reid, and Christopher Spirito. 2012. “Conceptual Framework for Cyber Defense Information Sharing within Trust Relationships.” Paper presented at the 2012 4th International Conference on Cyber Conflict, Tallinn, Estonia, June 5–8, 2012

Fleming, Matthew H., and Eric Goldstein. *Metrics for Measuring the Efficacy of Critical-Infrastructure-Centric Cybersecurity Information Sharing Efforts*. Washington, DC: Homeland Security Studies and Analysis Institute, 2012.

Fu, Xiao. “The Influences of Budgetary System in a Selection of Large Chinese Companies in the Industry of Electronic Household Appliances.” Master’s thesis, Durham University, 2012. http://etheses.dur.ac.uk/3644/1/Xiao_Fu_Upload_Thesis.pdf?DDD2+. Durham University, http://etheses.dur.ac.uk/3644/1/Xiao_Fu_Upload_Thesis.pdf?DDD2+.

Gattuso, James L. *Ensuring Cybersecurity: More Red Tape is Not the Answer* Washington, DC: The Heritage Foundation, June 5, 2012. http://www.heritage.org/research/reports/2012/06/cybersecurity-and-red-tape-more-regulations-not-the-answer.

Gonsalves, Antone. “How Retailers Can Boost Security through Information Sharing.” *CXO Media.* Accessed August 21, 2014. http://www.csoonline.com/article/2156060/data-protection/how-retailers-can-boost-security-through-information-sharing.html.

Goodman, Seymour E. and Herbert S. Lin, eds. *Toward a Safer and More Secure Cyberspace*. Washington, DC: The National Academies Press, 2007.

Government Accountability Office. *Cybersecurity National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented* (GAO-13-187.) Washington, DC: Government Accountability Office, February 2013.

———. *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*. (GAO 10–338). Washington, DC: Government Accountability Office, 2010.

Huberman, Michael and Matthew B. Miles. *The Qualitative Researcher's Companion* Thousand Oaks, CA: SAGE, 2002.

Inserra, David, and Paul Rosenzweig. *Cybersecurity Information Sharing: One Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace*. Washington, DC: Heritage Foundation, April 1, 2014.

iSight Partners. 2014. *What Is Cyber Threat Intelligence and Why Do I Need It?* Dallas: iSIGHT Partners, 2014.

Janczewski, Lech and Andrew M. Colarik. *Cyber Warfare and Cyber Terrorism*. Hershey, PA: IGI Global, 2008.

Lapointe, Adriane. *Oversight for Cybersecurity Activities: Why Intelligence Policies Won't Work, and What Kind of Approach W*ill. Washington, DC: Center for Strategic and International Studies, n.d.

Liu, Edward C., Gina Stevens, Kathleen Ann Ruane, Alissa M. Dolan, and Richard M. Thompson. *Cybersecurity: Selected Legal Issues* (CRS Report No. R42409). Washington, DC: Congressional Research Service, 2012.

Liu, Peng and Amit Chetal. "Trust-Based Secure Information Sharing between Federal Government Agencies." Journal of the Association for Information Science and Technology 56 (2005): 283–298.

Mandiant. *APT1 Exposing One of China's Cyber Espionage Units*. Alexandria, VA: Mandiant, 2013.

Markle Foundation Task Force. *Nation at Risk: Policy Makers Need Better Information to Protect the Country*. New York: Markle Foundation, March 2009.

Marsh, Stephen and Mark R. Dibben. "Trust, Untrust, Distrust and Mistrust–an Exploration of the Dark (Er) Side." In *Trust Management*, 17–33. New York: Springer, 2005.

Mickelberg, Kevin, Neal Pollard, and Laurie Schive. *2014 U.S. State of Cybercrime*, London: PricewaterhouseCoopers, June 2014. http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf.Miles, Matthew B. and A. Michael Huberman. *Qualitative Data Analysis: An Expanded Sourcebook.* Thousand Oaks, CA: SAGE, 1994.

Miller, Jason. "DHS Finds Classified Cyber Sharing Program Slow to Take Off." *Federal News Radio*. Accessed October 5, 2013. http://www.federalnewsradio.com/index.php?nid=851&sid=3356694.

Mitre. "Structured Threat Information eXpression — STIX A Structured Language for Cyber Threat Intelligence Information." Accessed December 2, 2013. http://measurablesecurity.mitre.org/docs/stix-intro-handout.pdf.

———. "Cyber Information-Sharing Models: An Overview." Accessed February 12, 2014. http://www.mitre.org/sites/default/files/pdf/cyber_info_sharing.pdf.

Moriarty, Kathleen. *Transforming Expectations for Threat-Intelligence Sharing.* Hopkinton, MA: EMC, 2013.

National Commission on Terrorist Attacks upon the United States. *The 911 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States.* Washington, DC: U.S. Government Printing Office, 2004.

National Infrastructure Advisory Council. "Executive Order and PPD-21 Working Group Recommendations for Maximum Engagement Including the Cybersecurity Framework, in Reducing Cyber Risks to Critical Infrastructure." September 4, 2013, http://www.dhs.gov/sites/default/files/publications/WG%20Adoption%20Recomendations.pdf.

NATO. "Multinational Experiment 7 Outcome 3—Cyber Domain Objective 3.2 Information Sharing Framework 22 January 2013." Accessed September 15, 2014. http://csrc.nist.gov/cyberframework/rfi_comments/dod_js_j7_part_2_022713.pdf.

Nelson, Rick and Wise, Rob. "Homeland Security at a Crossroads: Evolving DHS to Meet the Next Generation of Threats." Center for Strategic and International Studies, February 1, 2013. http://csis.org/publication/homeland-security-crossroads-evolving-dhs-meet-next-generation-threats.

Ngoma, Sylvester. "Vulnerability of IT Infrastructures: Internal and External Threats," Congo Vision. Accessed September 13, 2014. www.congovision.com/IT-Security-Pub.pdf, congovision.com.

Nicolaou, Andreas I. and D. Harrison McKnight. "Perceived Information Quality in Data Exchanges: Effects on Risk, Trust, and Intention to Use." *Information Systems Research* 17, no. 4 (2006): 332–351.

NIST. “NIST Roadmap for Improving Critical Infrastructure Cybersecurity.” Accessed August 2, 2014. http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf.

———. “Summary of the Privacy Engineering Workshop at the National Institute of Standards and Technology April 9–10, 2014.” Accessed August 2, 2014. http://www.nist.gov/cyberframework/upload/privacy-workshop-summary-052114.pdf.

Nyswander Thomas, Rachel. ,*Securing Cyberspace through Public-Private Partnership A Comparative Analysis of Partnership Models*. Washington, DC: Georgetown University, May 2012.

Office of the Director of National Intelligence. *Information Sharing Environment 2014 Annual Report to the Congres*s. Washington, DC: Office of the Director of National Intelligence, 2014. http://www.ise.gov/annual-report/section4.html.

———.*United States Intelligence Community Information Sharing Strategy*. Washington, DC: Office of the Director of National Intelligence, Feb. 22, 2008.

O’Neill, Maureen. “NVivo Toolkit.” QSR Corporation. Accessed April 19, 2014. http://explore.qsrinternational.com/nvivo-toolkit.

Ponemon Institute *Exchanging Cyber Threat Intelligence: There has to be a Better Way* Traverse City, MI: Ponemon Institute, 2014

PricewaterhouseCoopers. *Why You Should Adopt the NIST Cybersecurity Framework* London: PricewaterhouseCoopers, May 2014. http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf.

———. “Using NVivo for Qualitative Research.” NVivo 10 for Windows Help. Accessed June 30, 2014. http://help-nv10.qsrinternational.com/desktop/concepts/using_nvivo_for_qualitative_research.htm.

Rak, Adam. 2002. “Information Sharing in the Cyber Age: A Key to Critical Infrastructure Protection.” *Information Security Technical Report* 7, no. 2 (June 2002).

Relyea, Harold C. 2004. “Homeland Security and Information Sharing: Federal Policy Considerations.” *Government Information Quarterly* 21 (4): 420–438.

Riley, Michael, Elgin, Ben, Lawrence, Dune and Matlack, Carol. “Target Missed Warnings in Epic Hack of Credit Card Data.” *BusinessWeek*, March 13, 2014. http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

Rinaldi, Steven M. *Sharing the Knowledge: Government-Private Sector Partnerships to Enhance Information Security*. Colorado Springs, CO: USAF Institute for National Security Studies, 2000.

Robinson, Neil, and Emma Disley. *Incentives and Challenges for Information Sharing.* Heraklion, Greece: European Network and Information Security Agency, 2010.

Seigneur, Jean-Marc and Adam Slagell, eds. *Collaborative Computer Security and Trust Managemen*t. Hershey, PA: Information Science Reference, 2009.

Sekerka, Leslie E., Roxanne Zolin, and Cary Simon. *Rapid Transformation in a Dual Identity Defense University*. Monterey, CA: Naval Postgraduate School, 2005.

Singer, P. W. and Allan Friedman. *Cybersecurity and Cyberwar What Everyone Needs to Know*. New York: Oxford University Press, 2014.

Sinkovics, Rudolf R. and Eva A. Alfoldi. 2012. "Facilitating the Interaction between Theory and Data in Qualitative Research using CAQDAS," in *Qualitative Organizational Research: Core Methods and Current Challenges*, edited by Gillian Symon and Catherine Cassell. London: SAGE, 2012.

Smythe, Tiffany C. *Assessing the Impacts of Hurricane Sandy on the Port of New York and New Jersey's Maritime Responders and Response Infrastructure* Boulder, CO: Natural Hazards Center, 2013.

Sutton, David. 2013. "The Issue of Trust and Information Sharing and the Question of Public Private Partnerships." In *Critical Information Infrastructure Protection and Resilience in the ICT Sector* (Hershey, PA: IGI Global, 2013), 258–276.

Symantec Corporation. *2013 Internet Security Threat Report, Volume 18*. Mountain View, CA: Symantec Corporation, 2013.

Titch, Steven. "U.S. Cybersecurity Policy: Problems and Principles." The Heartland Institute, August 1, 2013., http://heartland.org/policy-documents/us-cybersecurity-policy-problems-and-principles.

Tor, Avishalom and Amitai Aviram. "Overcoming Impediments to Information Sharing." Alabama Law Review 55, no. 2 (Winter 2004): 231–279.

Verizon. *2013 Verizon Data Breach Investigation Report.* New York, Verizon, 2013.

Verton, Dan. "NSA Leaks Threaten Global Cybersecurity Information Sharing." *FedScoop*, October 16, 2013. http://fedscoop.com/nsa-leaks-threaten-global-cybersecurity-information-sharing/.

White House, The. "National Security Council Cybersecurity." Accessed August 1, 2013. http://www.whitehouse.gov/cybersecurity.

———. *National Strategy for Information Sharing and Safeguarding*. Washington, DC: The White House, December 2012.

———. "Presidential Policy Directive—Critical Infrastructure Security and Resilience," February 21, 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Whittaker, Zack. "Former NSA Executive: Snowden Leaks Caused 'Significant Disservice' to the Internet." *ZDNet*, April 24, 2014, http://www.zdnet.com/former-nsa-deputy-director-snowden-leaks-caused-significant-disservice-to-the-Internet-7000028746/.

Zegart, Amy B. *Spying Blind: The CIA, the FBI, and the Origins of 9/11*. Princeton, NJ: Princeton University Press, 2009.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California