# MANAGING CYBERSECURITY AS A BUSINESS RISK FOR SMALL AND MEDIUM ENTERPRISES

by
Stephanie K. Chak

A thesis submitted to Johns Hopkins University in conformity with the requirements for the degree of Master of Arts in Government

Baltimore, Maryland
May, 2015

## Abstract

Cyberspace has become the “Wild West” of business opportunities for companies. The explosion of growth opportunities has also created substantial cyber insecurity for such companies. Large companies have the budget and resources to manage cybersecurity risks with the ability to hire experts to provide guidance and technology to address problems on a large corporate scale. Small and medium sized enterprises (SME), on the other hand, lack the funding, knowledge, and human capital to sufficient defend itself against the various criminals. This research analyzes three solutions for some of the major categorical problems for SMEs looking to manage cybersecurity risks without necessarily large investments in only highly technical solutions which include community policing for broad cooperation within industries, cyber insurance, and cyber hygiene. The research was based on literature review on existing literature including substantial government policy, and openly available information available on the Internet. Research yielded the necessity of adopting solutions beyond technology in order to improve security and resilience for SMEs. The proposed solutions are ideally applicable under specific scenarios for SMEs. Broad adoption may not yield the necessary security or resilience for companies without a clear understanding of its existing security strategy.

Thesis readers: Dorothea Wolfson and Benjamin Ginsberg

# Table of Contents

## Introduction

The topic of cybersecurity or rather insecurity in cyberspace has been a popular topic in the media and on Capitol Hill. Most of the attention has focused on high-profile data breaches and government mandates with little attention to possible solutions for mitigating such issues. Currently, the legal framework for managing cyberspace is weak (such as the Council of Europe's Cybercrime Treaty) with most companies relying on proprietary approaches towards cybersecurity. In the private sector, large corporations have the resources and funds to manage its individual cybersecurity risks and policies and respond to incidents. However, small and medium enterprises (SME) are less likely to have the same kind of budget and resources to manage their cybersecurity risks effectively while they are more likely to be targeted by criminal hackers. Companies will have to continue to rely on proprietary measures for cybersecurity while the overall framework to manage cybersecurity and cybercrimes are formulated.

The US government is in progress to create a voluntary framework through the recently published Executive Order (EO) 13636 as a directive to create a voluntary framework for securing US critical infrastructure in cyberspace; it is an addition to the US Presidential Directive 54 for the security of critical infrastructure. It is a rational mandate because companies own most of the country's infrastructure and the security of the private sector infrastructure is listed as one of the priorities for the national security. While the lack of the specific guidance provides a positive environment to suggest a variety of possible solutions, there has not been many initiatives by either sector to decide which solutions to execute. It is difficult to maintain a balanced approach to creating a voluntary framework that fulfill the voluntary requirement from the private sector and maintain a high level of security sufficient for government standards.

The lack of initiative to experiment with solutions could mean that the policy problem of cybersecurity presented as something more daunting than it actually is in reality. Companies are operating in cyberspace without much awareness of possible risks. While large companies can operate without sharing resources, small and medium enterprises suffer from the lack of access to resources that can improve its security under smaller budgets. An obvious solution that has been repeatedly mentioned by cybersecurity third party providers is the necessity for increased investment in technology to improve security but is it the only way to improve security? Are there alternatives to investing more money into technology? This paper aims to evaluate novel concepts and tools that have not received much attention in aims to improve cyber risk mitigation (internally and collaboratively) and risk transfer. Some investment and time would be required to implement any of these recommendations, but SMEs would benefit greatly from the aggregation of cybersecurity data. The greater access to information can help companies devise internal strategies to improve its security while operating in cyberspace. Finally, those who wish to implement their risk transfer can do it confidently that it has

The thesis is comprised of three portfolio papers.

The first portfolio paper focuses on community policing in cyberspace. This paper consists of seven parts. This paper consists of seven parts. The first part will introduce essential definitions to understand policing in cyberspace. The second part of the paper will provide an overview of existing law enforcement involvement in policing cyberspace. The third part will be a literature review. The fourth section will examine the community policing concept. The fifth part of the paper will provide a methodology of necessary conditions for community policing and its application in cyberspace. The sixth part of the paper will explore the current challenges to adopting such an approach. The conclusion will discuss the importance of institutional leaders being open to changing policies with either completely new ideas or even adopting existing concepts. Evolution in cybersecurity is a necessity for both the private and public sectors to get ahead of criminals.

The second portfolio paper is about captive insurance as an alternative to existing commercial cyber insurance products. The first part will introduce the literature review and essential definitions to understand cyber insurance. The second part of the paper will provide an overview of existing role and state of cyber insurance in overall risk management for companies operating in cyberspace. The third part of the paper will review the roadblocks to developing a mature commercial cyber insurance market. Then this paper will examine captive insurance as an alternative to the commercial cyber insurance. The fifth part of the paper will explore three examples of companies and their respective experiences in managing the cyber-related incident and the role of insurance played in each case. In the conclusion, the paper will examine the analysis of the three case studies and the importance of risk management for SMEs.

The third paper is about cyber hygiene and its role in internally mitigating risk for end-users. This paper asks the following question: could the application of the concept “cyber hygiene” to an organization’s cybersecurity policy improve the effectiveness of addressing known virtual and physical vulnerabilities of a network’s security? The first part will present a survey of the existing research on human behavior in the context of cybersecurity. The second part will examine the current public literature of federal agencies and defense contractors. The third part will propose a definition of cyber hygiene. The fourth part is the conclusions and recommendations for future research.

# “Community Policing” in Cyberspace

## Introduction

The current cyberspace environment is analogous to the days of the Wild West. The Internet was created to expand opportunities for individuals to electronically communicate with each other without much regard to law and order. Indeed, the lack of order is one of the primary positive characteristics of the Internet, but it comes with fostering a somewhat lawless environment. Over time, more sophisticated communication networks have been created. Improved communications have created a multi-billion dollar global economy. Virtual network gateways used to protect transactions and other proprietary information has been insufficient against criminal hackers.[1] There are countless malevolent individuals and groups that operate freely in cyberspace while avoiding of the rule of law, such as organized criminal groups to hacktivist groups such as Anonymous and LulzSec. These groups have a variety of intentions, ranging from illegal financial gain to political aims. It is nearly impossible to maintain order over the Internet with the absence of a legal framework applied across most sovereign countries.

The development of a global legal framework for cybersecurity has been slow. Many countries have created their respective cybersecurity organizations to research and craft policy responses to network breaches and other illegal activity. It may address cybercrimes committed within a sovereign territory, but it does not adequately respond to crimes committed across physical borders. Currently, there are no international treaties that have been widely adopted to govern cyberspace and manage policing of cybercrimes.

[1] Sinrod, Eric J., and William P. Reilly. "Cyber-crimes: A practical approach to the application of federal computer crime laws." *Santa Clara Computer & High Tech. LJ* 16 (2000): 177.)

There have been attempts to adopt an international cybersecurity treaty such as the Council of Europe's Budapest Convention on Cybercrime, but the COE has been unsuccessful in widely ratifying the treaty outside of Europe. Currently, there are only four non-European country members (Australia, Dominican Republic, Japan, and the United States) that have ratified the treaty. [2] Member countries' domestic laws adhere to the treaty's requirements of prosecuting offenses against the confidentiality, integrity, and availability of computer data, systems, and hardware; child pornography; copyright infringement; and network security.[3] These laws show potentially allow the police to enforce laws based on the categories listed but do not provide specific guidance to law enforcement agencies on how to police these crimes committed in cyberspace. These types of crimes are similar to crimes in the real world but the assets involved or the method of how the crime was electronic-based. The lack of guidance for law enforcement has been both a blessing and a curse to law enforcement agencies. Most law enforcement agencies have been slow to develop procedures because of the lack of clarification, but there is potential for police to improve policing in cyberspace.

Large enterprises recognize that operating cyberspace have inherent risks and most if not all have allocated resources focused on minimizing the risk of operating in cyberspace. Large enterprises have sophisticated information technology and security departments to formulate IT policies, and trained experts for active monitoring of its networks for data breaches. Large companies' technology departments also have technical tools to manage internal network security. They are also likely to purchase

[2] "Treaty Office." *Council of Europe* . N.p., n.d. Web. 24 July 2013. <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>.

[3] "ETS No. 185 - Convention on Cybercrime." Council of Europe - Treaty Office. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (accessed August 6, 2013).

expensive memberships in public private partnerships such as information sharing and analysis centers (ISACs) to obtain high quality third party analysis and intelligence on potential threats. ISACs help inform companies about industry wide threats and share relevant information with government agencies. Large enterprises' access to the human capital and technology will mitigate some of the risks of operating in the gray area of cyberspace- internally and externally.

While large enterprises have taken steps to reduce the risk of operating in cyberspace, they are still vulnerable to becoming victims of cybercrimes. When these companies are victims of publicized cybercrimes, they experience significant financial repercussions.[4] The severity of damages stemming from cybercrimes has had varying effects on companies. Indirect losses are hard to quantify but large publically traded companies such as Target and Home Depot have experienced significant downward pressure on the price of the stock after cybercrimes are publicly reported. Large multinational corporations are more likely to overcome direct losses from these crimes with vast balance sheets and potentially financial compensation from insurance.

Small and medium enterprises (SME) generally have fewer resources to mitigate risks of operating in cyberspace. SMEs are less likely to have skilled skilled IT employees, much less a dedicated IT department to formulate IT policies to mitigate breaches, and business continuity planning. The lack of skilled employees to champion the importance of risk mitigation will also affect investments in memberships such as ISACs. More often than not, SMEs are likely to contract out active monitoring to third party companies with turnkey software or simple anti-virus software. This can pose a risk

[4] Menn, Joseph . "Major Companies Keeping Cyber Attacks Secret from SEC, Investors: Report." Insurance Journal News. http://www.insurancejournal.com/news/national/2012/02/02/233863.htm (accessed December 4, 2013).

in itself that vulnerable software offered by third party companies are likely to add exposure to data breaches if vulnerabilities can be systemically exploited or defenseless against skilled hackers.[5] SME have smaller balance sheets or operating accounts to absorb direct losses stemming from cybercrimes. They are more likely to struggle from cybercrimes because they are also less likely to own adequate insurance to losses related to digital assets. While SMEs are less obvious targets, the assets and inherent vulnerabilities of SME can be attractive to criminal hackers.

The individual losses and recovery costs experienced by companies are significant enough to warrant attention to improving mitigation of the risks of operating in cyberspace. Ponemon Institute conducted a study that showed a US company that was a cybercrime victim experienced a loss on average of $8.9 million, an increase of 6% from 2011 and up 38% from 2010. [6] The cost comes from a combination of loss of intellectual property or confidential information, business disruption, lost revenue, and equipment and/or system damages. On average, each cleanup for a security breach cost $592,000, a 42% increase from the average reported for 2011 cleanup cost of $416,000. [7] While these losses have not deterred companies from operating in cyberspace, this kind of unexpected loss is significant to the bottom line for many SMEs.

This paper will argue that the adaptation of the real world community policing can be applied in cyberspace to increase legal order and a sense of security for all companies, especially SMEs. While the perception of security is not the same as real security, the

[5] Weise, Elizabeth. "Antivirus Software Powerless against Sony Hackers." USA Today. December 6, 2014. Accessed February 3, 2015. http://www.usatoday.com/story/tech/2014/12/06/sony-attack-new-era-nuclear-option/19963063/.

[6] "2012 Cost of Cyber Crime Study: United States." Ponemon Institute. www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf (accessed July 31, 2013).

[7] Ibid.

minimum perception will beget a continuous commitment to maintaining security and cooperation towards mitigating risk by voluntary cooperation by companies. The increased cooperation between companies and law enforcement, on the whole, will increase the ability the law enforcement can better police cyberspace over time. Prior research shows that the community policing can possibly solve cybercrimes on a global scale, but this paper will focus on crimes that affect the private sector in the United States.

This paper consists of seven parts. The first part will introduce essential definitions to understand policing in cyberspace. The second part of the paper will provide an overview of existing law enforcement involvement in policing cyberspace. The third part will be a literature review. The fourth part will examine the community policing concept. The fifth part of the paper will provide a methodology of necessary conditions for community policing and its application in cyberspace. The sixth part of the paper will explore the current challenges to adopting such an approach. The conclusion will discuss the importance of institutional leaders being open to changing policies with either completely new ideas or even adopting existing concepts. Evolution in cybersecurity is a necessity for both the private and public sectors to get ahead of criminals.

## Definitions

This paper focuses on the application of ‘community policing’ in cyberspace as a public and private sector partnership with clearly delineated roles for both parties. It does not include police utilization of cyberspace to investigate crimes committed in the physical realm. While the utilization of electronic evidence found in cyberspace is under development, it will not be within the paper's scope. The primary focus of the paper will focus on electronic crimes committed against companies in cyberspace and a proposal of redefining information sharing and cooperation for between the public and private sectors. The definitions will help understand the terminology that is relevant to the medium, some of the cybercrimes, and the definition 'community policing.'

*Cyberspace* is a term that is used interchangeably with the term- Internet. The Internet is comprised of physically connected networks around the world, many have viewed cyberspace as the physical identity for computer-mediated communications.[8] It should not be confused with virtual reality where individuals adopt telepresence and function in a separate world. [9] Real world threats are more likely to be visible, whereas cyberspace threats/crimes may not be all that apparent to users and organizations. There are a number of terms typically used when discussing technical activities used in committing cybercrimes.

An important term to attempt to define is cybercrime itself. There is a variety of definitions of cybercrime. Surprisingly in the US, there is no official definition of cybercrime that distinguishes crimes committed in cyberspace and the real world. [10] Cybercrimes are often used interchangeably with the Internet or other technology related crimes.[11] The most widely accepted definition would arguably originate from the Council of Europe since it is currently the most widely adopted treaty on cybercrime. Council of Europe's Convention of Cybercrime focuses on "crimes committed via the Internet and

[8] Joinson, Adam N. "Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity." *European Journal of Social Psychology* 31, no. 2 (2001): 177-192.

[9] Steuer, Jonathan. "Defining virtual reality: Dimensions determining telepresence." *Journal of communication* 42, no. 4 (1992): 73-93.

[10] Finklea, Kristin M. , and Catherine A. Theohary . "Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement." Federation of American Scientists. http://www.fas.org/sgp/crs/misc/R42547.pdf (accessed December 9, 2013).

[11] Ibid.

other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security." [12]

The Convention of Cybercrime provides guidance on the types of crime but can also be too constrained in its definition. Thomas and Loader viewed cybercrimes as "computer-mediated activities that are either illegal or considered illicit by certain parties and conducted through global electronic networks." [13] The definition by Thomas and Loader is almost sufficient for identifying the tangible and intangible related to cyber-crimes except that it limits the type of equipment that can be used to commit these activities such as cell phones. Gordon and Ford expand on the definition by broadening the type of equipment used in cybercrimes by defining cybercrime as "any crime facilitated or committed using a computer, network, or hardware device." [14] The last two definitions are more appropriate in broadly understanding the types of activities that can be considered as cybercrimes. The COE's definition is limiting in comparison, but it does provide some guidance by listing specific activities that qualify as cyber-crimes.

There are endless definitions for cybercrime because there is a variety of aspects to consider about cybercrime. The components of a cybercrime vary in three ways of 1) In some cybercrimes that computers or data are the targets. 2) Computers or digital technologies used as tools for committing cybercrimes. 3) Technological devices carry evidence when used as tools for committing cybercrimes.[15] Some real world crimes use technology to steal information, such as point of sale skimming. It occurs when a device

[12] "Summary of the Convention on Cybercrime (CETS No. 185)." Council of Europe - Treaty Office. http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm (accessed August 4, 2013).
[13] Loader, Brian D., and Douglas Thomas, eds. *Cybercrime: Security and surveillance in the information age*. Routledge, 2013.
[14] Gordon, Sarah, and Richard Ford. "On the definition and classification of cybercrime." *Journal in Computer Virology* 2, no. 1 (2006): 13-20.
[15] Finklea, Kristin M. , and Catherine A. Theohary . "Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement." Federation of American Scientists.

is placed on top or replacing an existing card slot on a credit card reader or ATM. The device copies the magnetic stripe information and pin information, information is then broadcasted to criminals.[16] Information can then be burned onto blank cards to withdraw money or sold online in batches.

The complexity of these crimes can vary on the tools used to commit such crimes. Some of them can be as simple as accessing illegal content such as child pornography or illegally downloading copyrighted material such as music and movies. Other crimes can be very sophisticated such as creating botnets and distributed denial of service (DDoS.) These two digital tools require a sophisticated knowledge of utilizing computers and programming. Some of the tools, such as botnets and DDoS, are now sold as crime as a service to traditional criminals or criminal groups. These criminal users can lease the software for any period of time while the software is maintained by hackers.[17] This kind software has empowered groups that have the ambition to control computers illegally for the aim of stealing money or holding companies hostage without the complex technology knowledge to implement such software.

*Phishing* is a scheme to obtain personal identifiable or financial information deceitfully from unsuspecting individuals. This is usually executed by large batches of fraudulent emails purportedly sent from legitimate organizations, to potential victims requesting information. Some criminals are sophisticated enough to locate electronically stored documents with the victim’s signature and replicated phone numbers when service providers attempt to confirm the victim’s information as experienced by firms such as

[16] Bid.

[17] Sood, Aditya K., and Richard J. Enbody. "Crimeware-as-a-service—a survey of commoditized crimeware in the underground market." *International Journal of Critical Infrastructure Protection* 6, no. 1 (2013): 28-38.

Morgan Stanley in Washington DC. This is a serious problem, especially for financial services firms that manage large amounts of money because there are times that good compliance measures cannot easily overcome the sophisticated criminal's ability to provide evidence to confirm authorizations to transfer money.

Distributed denial of service (DDOS) is an attack by hackers on computers and specific networks to prevent legitimate users from accessing the intended information. [18] The most common tactic to carry out such attack is by flooding the target with information that overwhelms the targeted website is no longer accessible to the intended users. For some organizations that experience this kind of crime when a malicious hacker(s) attempts to subvert the organization by prevent legitimate users from accessing its website. US banks such as Bank of America, Citigroup, Wells Fargo, and others experienced this in the fall of 2013 when their websites faced major disruptions.[19] Cyber experts such as James Lewis and US intelligence officials believed this campaign was organized by Iran.[20] These types of attacks are viewed as a form of a political message.

SQL injection is a type of attack that undermines the relationship between a website and its supporting database. The Code specifically developed for a SQL injection will deceive the database system into executing malicious code.[21] The action is a combination of exploiting database vulnerabilities, over-elevated permissions of certain

[18] US CERT. "Security Tip (ST04-015)." Understanding Denial-of-Service Attacks. http://www.us-cert.gov/ncas/tips/ST04-015 (accessed March 24, 2014).
[19] Perlroth, Nicole, and Quentin Hardy. "Bank Hacking Was the Work of Iranians, Officials Say." The New York Times. January 8, 2013. Accessed February 4, 2015. http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?pagewanted=1&_r=0.
[20] Ibid.
[21] "SQL Injection." US-CERT. http://www.us-cert.gov/security-publications/sql-injection (accessed March 26, 2014).

users, unsanitized/untyped user input, and/or software (database) vulnerabilities. [22] These type of attacks can occur even when there are no known vulnerabilities in a database and much more complex than a typical security patch because it can hide within the countless amounts of information. *"Community policing"* is a concept that emphasizes working partnerships between police and communities to enhance a sense of security and trust in order to reduce crime. The definition by the Department of Justice is "a philosophy that promotes organizational change strategies, which support the systematic use of partnerships and problem-solving techniques, to proactively address the immediate conditions that give rise to public safety issues, such as crime, disorder, and fear of crime."[23] The concept focuses on a collaborative approach involving multiple stakeholders in order to resolve conditions that can lead to the sense of insecurity. One of the important components of a thriving community is the business community. Businesses require a secure environment in order to conduct transactions.

*Information Sharing and Analysis Centers* are an example of a public-private partnership created to encourage dialogue between industry and the government. These organizations gather, share and disseminate information related to both physical and cyber threats to companies within a specific sector and the federal government. [24] ISACs are private organizations dedicated to the fifteen industries considered to be critical infrastructure by the federal government. It was voluntarily created by companies within their respective critical infrastructure sector in response to Presidential Decision Directive

[22] Ibid.

[23] "COPS Office: What is Community Policing?." COPS Office. http://www.cops.usdoj.gov/Default.asp?Item=36 (accessed March 10, 2013).

[24] Relyea, Harold C., and Jeffrey W. Seifert. "Information Sharing for Homeland Security: A Brief Overview." LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE, 2005.

63. *Critical infrastructure* is comprised of assets, systems, and networks, physical or virtual, which are vital to the country that incapacitation or destruction would cripple the country's national security.[25] Approximately 85% of the country's critical infrastructure is owned by the private sector that can be categorized into 16 sectors as organized by the Presidential Policy Directive 21. [26] There are 16 Information Sharing and Analysis Centers in the United States. Most US companies fall into some critical infrastructure, and therefore they qualify to join a relevant sector ISAC.

ISACs' missions are focused on the real time threats of its respective sectors. The ISACs have developed independently to serve the respective needs of the industries. ISACs were formed by one of two ways. One was legal incorporation and independent operations or contracting operations out to a security firm. [27] Banking, information, water, oil and gas, railroad, and mass transit industries used the approach. The second model was utilizing an existing organization that coordinated government-industry efforts and added critical infrastructure protection to the mission of the group. Electric power uses the North American Electricity Reliability Council, and the telecommunications sector uses the National Coordinating Center. [28] These organizations have developed unique management structures and services tailored to their respective sectors. ISAC funding has varied with some have received funding from government agencies either for start-up purposes or ongoing funding or others completely self-sufficient. Some ISACs have formed an umbrella group called the ISAC Council to help facilitate additional

[25] "What Is Critical Infrastructure?." Homeland Security. http://www.dhs.gov/what-critical-infrastructure (accessed December 7, 2013).

[26] Ibid.

[27] Moteff, John D. *Critical infrastructures: Background, policy, and implementation*. DIANE Publishing, 2010.

[28] Ibid.

coordination. [29] The manner in which these organizations have progressed from its funding to organization shows that the mission is very much focused on the gathering, sharing, and disseminating threats to the sector members. However, it is not necessarily clear these organizations have a systemic approach to mitigating cybercrime threats in a meaningful manner.

These organizations are charged with mandates to help coordinate communication and information sharing between the private sector and federal agencies regarding the security of all types including cyber. One of the critiques of these organizations is that there is no clear delineation of responsibilities between the ISACs and federal agencies. Though this cannot be completely the fault of the ISACs or federal agencies, a GAO report identifying that the DHS is responsible for a coordination strategy. This is one of the ongoing issues facing public-private partnerships, many federal agencies are tasked with mandates without guidance on how to proceed. It is difficult to clearly to delineate the roles that each organization (governmental or private-partnerships) plays in ecosystem of cyberspace security.

### Current Law and Order in Cyberspace

There is no explicit US national strategy for policing cybercrimes but there are a number of national level organizations that list cybercrime as one of its objectives. The Federal Bureau of Investigation was listed in the President's National Strategy to Secure Cyberspace in 2003 as the leading federal law enforcement agency in the United States in charge of investigating cybercrimes.[30] The US Secret Service is responsible for

[29] Ibid.

[30] "Addressing Threats to the Nation's Cybersecurity." FBI . http://www.fbi.gov/about-us/investigate/cyber/addressing-threats-to-the-nations-cybersecurity (accessed April 8, 2013).

investigating crimes that involve the financial infrastructure and payment systems. [31] The US Secret Service was mandated by the Patriot Act to establish a national network of Electronic Crimes Task Forces (ECTF.) These ECTFs are working partnerships with private industry, academia, local and state authorities, and prosecutors.[32] There are 25 ECTFs located in major cities all over the United States. In the private sector, ISACs are where member companies share anonymized information regarding the physical and cyber threats and vulnerabilities as directed originally by Presidential Directive 63 and later updated in Homeland Security Presidential Directive 7. [33] Domestic Security Alliance Council and InfraGard are both lead by the FBI to facilitate information sharing and cooperation between US companies and FBI and Department of Homeland Security (DHS.) [34] Other organizations related to cybersecurity such as the Homeland Security Information Network which is a communication network for sharing and analyzing real-time threat information at federal, state, and local law enforcement. US-CERT (U.S. Computer Emergency Readiness Team) publishes information on the latest computer-related vulnerabilities, threats, and information on how to respond.[35] These organizations have roles in information gathering, organizing, investigation, dissemination, and sharing but it is easy for the uninitiated in cyber security to be easily confused on exactly which organizations can help them in the event they experience a cyber-related incident.

Under the current policing regime in cyberspace, there have been some successful

[31] "Vision and Mission Statements." United States Secret Service. http://www.secretservice.gov/mission.shtml (accessed August 4, 2013).

[32] "Electronic Crimes Task Forces and Working Groups." United States Secret Service. http://www.secretservice.gov/ectf.shtml (accessed August 6, 2013).

[33] "About FS-ISAC." FS-ISAC : Financial Services. https://www.fsisac.com/about (accessed December 7, 2013).

[34] "Welcome to the Domestic Security Alliance Council." Domestic Security Alliance Council. http://www.dsac.gov/Pages/index.aspx (accessed December 21, 2013).

[35] Moteff, John D. *Critical infrastructures: Background, policy, and implementation*. DIANE Publishing, 2010.

indictments of criminal users. In July 2013, there was a very significant indictment for the largest known data breach. The US Secret Service led the investigation that led to the indictment by the New Jersey state attorney. Five individuals were listed in the conspiracy indictment. Four were Russian citizens-Vladimir Drinkman, Alexandr Kalinin, Roman Kotov, and Dmitriy Smilianets; and one Ukranian-Mikhail Rytikov. Drinkman and Kalinin respectively specialized in penetrating network security and accessing network systems. Kotov specialized in mining networks. Rytikov provided anonymous web-hosting services. Smilianets sold the stolen information and distributed the proceeds to the other conspirators. The conspirators were accused of penetrating the computer networks of the several largest payment processing companies, retailers, and financial institutions such as Heartland Payment Systems, JCP, Dow Jones, Visa Jordan, and Diners Singapore.

The group entered those corporate networks by identifying vulnerabilities in SQL databases and used those vulnerabilities in an SQL injection attack to gain entry. The group also left malicious code or malware to re-enter the compromised network easily. If the company's computer security removed the malware, the group would patiently and persistently attack until they regained entry into these networks.  The group stole usernames and passwords, personal identification information, credit and debit card numbers. The group stole a conservative estimate of more than 160 million card numbers. The group then sold the stolen credit card numbers and associated information in batches called “dumps” to resellers around the world. The buyers of these dumps would resell the dumps to other individuals or organizations either directly or through online forums. The cards and its associated information were charged different according to the country of origin; US cards were $10, European cards were $50, and Canadian cards were $15 each.

It took years for law enforcement to discover the group and the arrests of the members of the group were just as difficult. The conspirators proactively covered their tracks of their illegal activities. Rytikov allowed his clients to hack companies with the agreement that his company would not keep records of the group's online activities or communicate with law enforcement. The other defendants also communicated through private and encrypted communication channels. Some of the defendants attempted to meet in person to avoid law enforcement inception of their private communication.

The majority of the conspirators avoided arrest, but Smilianets was the easiest to trace out of the group because he was interacting with many people in order to sell the "dumps" of credit card information. He was already well known because of his high profile in Russia as the founder of a championship electronic gaming team. Law enforcement received some information about Smilianets travel to Europe with a friend. The friend was Drinkman who actively posted information about their trip on social media websites that law enforcement deduced where they were both staying.[36] Drinkman and Smilianets were both arrested on June 28, 2012. Smilianets was extradited to the United States on September 7, 2012 while Drinkman is still fighting extradition in the Netherlands. The rest of the group remains at large.

In an older case investigated by the FBI, the law enforcement agency successfully infiltrated a very exclusive black market forum called the "Dark Market." Criminals bought and sold stolen financial information, stolen login credentials, stolen credit card

[36] Claburn, Thomas. "Record-Setting Data Breach Highlights Corporate Security Risks." InformationWeek. http://www.informationweek.com/security/vulnerabilities-and-threats/record-setting-data-breach-highlights-corporate-security-risks/d/d-id/1110930? (accessed March 22, 2014).

information, and even tools to commit financial crimes in the Dark Market.[37] The electronic market was not an ordinary forum that anyone could join: members had to be vetted before operating in the black market. At its peak, the “Dark Market” had as many as 2,500 registered members. The FBI conducted a two-year undercover cybercrime investigation, working closely with the U.K.’s Serious Organised Crime Agency, the Turkish National Police, and the German Federal Criminal Police.[38] FBI infiltrated the “Dark Market” with an agent, named Master Splyntr, posing as cyber criminal and installing himself as the site administrator. The investigated ended in 2008 with 60 arrests around the world and prevented the $70 million in economic loss. [39] The founder of Dark Market, Renukanth Subramnian, was found guilty in a British court and ordered to serve 46 months for conspiracy to defraud and ten months for five counts of mortgage fraud. [40] It is not the most egregious case, but it highlights that criminals are enterprising types that are not just focused on hacking. These types of underground markets are perpetuating the availability of criminal software in cyberspace.

These prior examples are a small part of an asymmetrical environment where criminals continue to experience low barriers of entry to committing cybercrimes and relatively low risk of arrest and prosecution. There are a number of government organizations responsible for managing cybersecurity on a broad scale, but companies carry the burden of spending significant sums of money to defend against internal and

[37] "Dark Market Takedown." FBI . http://www.fbi.gov/news/stories/2008/october/darkmarket_102008 (accessed April 8, 2013).

[38] Ibid.

[39] Chabinsky, Steven. "Statement Before the Senate Judiciary Committee, Subcommittee on Terrorism and Homeland Security Washington, D.C.."*FBI*. N.p., 17 Nov. 2009. Web. 24 Mar. 2014. <http://www.fbi.gov/news/testimony/preventing-terrorist-attacks-and-protecting-privacy-rights-in-cyberspace>.

[40] "Organiser of Darkmarket fraud website jailed." BBC News . http://news.bbc.co.uk/2/hi/uk_news/8539680.stm (accessed August 6, 2013).

external threats to the network security. Cyber crimes perpetuate because it does not require as many resources or technical knowledge to exploit the weaknesses of an organization, although groups attempting to commit crimes on an enterprise level usually include expert hackers with a variety of technical skills to commit crimes in an organized fashion. The numbers of cyberspace crimes continue outpace the number of law enforcement officers who are skilled enough to track them down.[41] The reward for committing crimes to earn relatively easy cash or bragging rights to penetrating and interrupting networks for a political purpose such as Anonymous will continue to perpetuate crimes with political goals. Many of the criminals operate in countries that allow impunity, such as Eastern European countries, Russia, and China. The combination of the relative low risk and high rewards will continue to perpetuate cybercrimes unless law enforcement policies change.

The current policing of criminals who commit cybercrimes have been ineffective. Most continue to commit crimes without fear of prosecution and arrest. The publicized arrests and prosecutions of criminal hackers are exceptions to the norm. Due to the limited time and resources available to investigate crimes, of any type, are usually utilized by the most economically significant cases that feature large companies as victims rather than lesser known SMEs. There is a shortage of law officers trained in the technical aspects of the cybercriminal world and forensics experts in cybercrimes. The lack of qualified professionals to investigate cybercrimes will continue to benefit criminals. If investigations are initiated, it can take months if not years to complete as the prior examples demonstrated. Law enforcement involved in undercover investigations

[41] Anderson, Ross, Chris Barton, Rainer Böhme, Richard Clayton, Michael van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. "Measuring the Cost of Cybercrime." In *WEIS*. 2012.

need time to build the relationships with the small circles of criminals involved in the cybercrimes. Even arresting criminals can take time with time, to locate criminals and extradite from the country where the criminal is arrested and send them to the country with the criminal indictment. Collecting evidence that can be admissible in court is still under development. Law enforcement are starting to increase training and hiring of individuals experienced in dealing with such crimes, but it is not at a pace that will come close to meeting the demand of investing most cybercrimes.

Current policing within cyberspace shows a lack of a cohesive strategy that clearly defines the roles and responsibilities of the private sector companies and the law enforcement. The largest companies that have significant resources are more likely to institute tools that mitigate a fair amount of risk. While SMEs lack the same kind of resources and human capital to mitigate risk and plan for unexpected cyber incidents. Companies within industries lacking in coordination of information sharing and responsiveness unknowingly experience systemic threats if there are state-sponsored criminal hackers who can operate with impunity. The lack of minimum security requirements within respective industries places an outsized burden on law enforcement to maintain security or at least the perception of security in cyberspace. The limited resources of law enforcement cannot sufficiently carry the burden and that its efforts need to focus on investigating in a manner that is effective in coordinating with the private sector. The cooperation and sufficient coverage of arrests will improve the perception of security towards raising the cost-benefit analysis for criminals who consider in engaging criminal activities in cyberspace.

## Literature Review

The concept of community policing in the real world has explored from many angles, but there is limited existing research on the concept of "community policing" in the cyberspace realm. The available research shows a number of major viewpoints on police involvement in cyberspace.

One of the concepts is reliance on private self-help, where individuals are incentivized to protect themselves against crime. [42] Neal Katyal wrote about the concept of "community" self-help, where there is a greater emphasis on the precautions taken by a community rather than by individuals or completely relying on law enforcement. Katyal states that each camp will have to admit that its method alone is ineffective against crime: Lone actors who try to stop crimes by themselves cannot be trusted, and their success in reducing crime will also increase the amount of fear of crimes. Law enforcement crackdowns on crime can fray a community, possibly producing counterproductive results.[43] Moreover, in a complete self-help model, wealthier individuals who can afford to protect themselves would transfer some of the crime to their poorer neighbors. As an alternative, Katyal supports cooperative prevention over prosecution or retribution. In the approach recommended by Katyal, local "realspace" neighborhoods would coordinate with law enforcement as opposed to both parties reacting independently of each other. Community self-help would ideally balance the goals of formal and informal enforcement of laws and socially accepted norms. The term neighborhood was not specifically defined by the author. It can be a confined area where a group of people living in close vicinity of one another such as a gated community as referred to by the author. Kaytal recommends that community policing in realspace has potential in

[42] Katyal, Neal. "Community Self-Help." *JL Econ. & Pol'y* 1 (2005): 33.
[43] Ibid.

lowering crime rates and recommends exploring the concept in cyberspace and should look at realspace examples of community policing for guidance.

Benjamin Jones took a different approach with the concept of community policing in cyberspace. He argued that a community approach by programmers and developers to create open source software code especially in the operating system and Internet browser markets that will deter cybercrimes.[44] The success of the open source software will be distributing information across the entire community of software users. There are instances of these projects such as GitHub, currently the largest open source community to share code between software developers.[45] While this concept will more likely work for less sophisticated cybercrimes across the entire cyberspace such as ransomware-software that will hold the computer functionality hostage until the user pays a ransom.[46] The paper disagrees that corporations and governments are less likely to participate in such a proposition since it does not sufficiently address crimes such as targeted phishing.

A prominent scholar in cybercrimes, David Wall, argued that police will have to cooperate with various groups such as Internet user groups, virtual environment managers, Internet service providers, corporate security organizations, etc involved in enforcing norms and laws.[47] Wall identified a larger ecosystem of organizations that enforce norms and laws in cyberspace. Wall argued that police forging relationships with the other cooperative partners would improve policing in cyberspace. He also argued that governance should be configured to assist and strengthen the Internet’s natural inclination

[44] Jones, Benjamin R. "Comment: Virtual neighborhood watch: Open source software and community policing against cybercrime." *The Journal of Criminal Law and Criminology* (2007): 601-629.
[45] "Build software better, together.." GitHub. https://github.com/ (accessed January 9, 2014).
[46] Gazet, Alexandre. "Comparative analysis of various ransomware virii." *Journal in computer virology* 6, no. 1 (2010): 77-90.
[47] Wall, David S. "Policing cybercrimes: Situating the public police in networks of security within cyberspace." *Police Practice and Research* 8, no. 2 (2007): 183-205.

to police itself.[48] The desire to automate policing may evolve from a ‘disciplinary society’ to a ‘control society’ where actions can be analyzed for predicting criminal behavior.[49] This paper disagrees that policing will become sophisticated enough in the near term to solve crimes committed by talented hackers. While Wall was able to identify a larger ecosystem of interested parties, there is not enough depth on possible specifics on how to forge productive relationships with these disparate groups to improve cyberspace policing.

These authors make important contributions by presenting in-depth focus on aspects of the overall community policing concept on a very broad scale. In an attempt to solve a broad problem with broad solutions will not adequately solve anyones’ problems. The lack of specificity in the responsibilities for user groups reduces the effectiveness of improving security in cyberspace. It is dangerous because it will take away resources from solutions that can accomplish less but in a more effective manner.

## Understanding Criteria for Successful “Community Policing”

The components of successful “community policing” involve a working relationship with regular communication with local police officers, residents, and community stakeholders such as community leaders, media, and business owners. There are necessary attributes to any successful “community policing” relationship, including: empowerment of the community; belief in a broad police function; reliance of police on citizens for authority, information, and collaboration; specific tactics targeted at particular problems unique to the community; and decentralized authority to better respond to

[48] Ibid.
[49] Ibid.

neighborhood needs.[50] The increased communication between both parties and reorientation from a focus on internal police performance metrics to the perception of safety within the neighborhood should be considered again.

The implementation of “community policing” should be a starting point to build a cooperative relationship between the law enforcement and the community. So the two parties can co-create an approach towards solving the community’s problems. Over time, the working relationship between the community and the police would ideally foster trust and an open environment for communication.[51] In an ideal situation, there is regular interaction between community stakeholders and local law enforcement. The community can communicate what it perceives as threats to its safety and law enforcement can create and implement strategies to fulfill those needs while also enabling the law enforcement agencies communicate potential threats identified through its intelligence gathering activities. The service-oriented approach should foster an environment perceived safe by all community stakeholders to function and thrive. Security considerations by a neighborhood may or may not be the same as the prior police metrics for performance. The increased perception of security will beget involvement from community members to share information to prevent further criminal incidents from affecting the rest of the community. The criteria for a successful “community policing” in cyberspace will follow a similar fashion to its real world counterpart. The criteria as follows:

- Participation from all stakeholders in the community
- Regular communication between the community and law enforcement

[50] "Community and Problem-Oriented Policing (OJJDP Model Program Guide)." Office of Juvenile Justice and Delinquency Prevention. http://www.ojjdp.gov/mpg/progTypesCommunityProblem.aspx (accessed March 12, 2013).

[51] Office of Community Oriented Policing Services. "Community Policing Defined." Department of Justice. www.cops.usdoj.gov/Publications/e051229476_CP-Defined-TEXT_v8_092712.pdf (accessed February 2, 2013).

- Collection and analysis of information from the community
- Decentralized authority for law enforcement to respond to the community's needs
- Resolve particular problems for the community
- Assess the effectiveness of the solutions

To apply the concept of community policing in cyberspace, it will require some adaptation due to its unique nature of cyberspace and its borderless environment. First, the definition of 'community' will focus on companies only rather than including individuals in cyberspace. The community aspect would the interactions within the ISACs. These types of organizations already exist and function as a conduit between companies and the federal government. It will not require significant additional investment in restructuring the infrastructure to support companies on a wider and more effective scale.

The complexity of attempting to police the cyberspace on a broad scale would take time to implement. The increased focus on sub-user groups rather than the broader population will improve the overall effectiveness of the solution because the needs will be better aligned when focused on sub industries. The lack of geographical constraints in cyberspace will limit the ability of the community policing through the local police. Law enforcement in the cyberspace context will focus on federal agencies rather than local police in order to better pursue criminals on a sustained basis and cooperation for extradition. Federal agencies will also have budgets and experience to hire or train technical experts and agents dedicated to policing cybercrimes.

### Can "Community Policing" be applied to Cyberspace?

The first requirement is to have participation from all stakeholders in the community, specifically the industry. Participation within the industry requires incentives to attract companies to invest in a group effort to combat cybercrimes. There are two approaches to incentivize companies to participate with 1) assurances that anonymized information shared will not break anti-trust rules or shared beyond its original purposes of technical analysis for criminal activities 2) financial incentives such as lower cyber insurance premiums or tax benefits for participating companies. The anonymous information shared with the insurance industry will provide more information to needed to calculate the actuarial risk of accepting an insured company's operating risk in cyberspace. Large and small-medium enterprises will be incentivized to participate on a broad scale. Large enterprises will benefit from the enhanced power of group sourced information and another layer of situational awareness of operating in cyberspace in addition to proprietary tools. SMEs will have access to better industrial and systemic threat analysis and additional information through wider participation that would not be easily attained on an individual basis. In order for the concept to be applied in cyberspace, high participation is a necessary. As companies of sall sizes experience cybercrimes, it will increase the likelihood that they will be self-motivated to join to mitigate the risk of experiencing additional cybercrimes.

Another aspect of successful community policing is the ability to identify clearly and articulate security problems for the community. In order to clearly identify problems for the community, the size of the community needs to be subdivided into a manageable size to identify problems that affect smaller groups accurately. Instead of focusing on the traditional smaller geographic neighborhood in traditional community policing, the concept can be applied by dividing the size of the broad industry into sub-groups within industries by similar risk and use patterns. Once companies have been grouped together based on similar operating and risk profiles, there will be aggregate continuous monitoring within the sub-groups. It allows ISACs to pool resources such as technical experts and to narrow the range of acceptable activity and highlight highly unusual activity within the sub-groups. The benefit of creating these sub-groups of member companies will not only include continuous monitoring for potential cybercrimes but also the ability to analyze continuous real-time activity for abnormal patterns. Continuous analysis could enable the identification of potential criminal activity within a sub-group of similar peers. ISAC technical specialists will analyze activity to establish a range of acceptable regular activity. Analysts can report if there are campaign attacks on subgroups of companies or if there are broader industry threats. The ISAC experts can offer a third party opinion of activity and forensic services after incidents are reported to the broad industry membership. Any potential cybercrime activity or threats will be reported to members of the affected sub-group and possibly to the broader industry ISAC. The ISAC can assist in reporting of the incident to the appropriate law enforcement organization while protecting the integrity of data as evidence.  A record of the cybercrime will be filed in the ISAC database will be built on the activity. Any future cybercrime activity will be compared to the existing database to examine whether it fits a pattern of cybercrime. It will help build up a repository of profiled but yet unidentified patterns of activity to be shared with law enforcement and prosecutors to investigate, identify, and indictment/arrest. Information shared with the appropriate law enforcement agencies will contribute to the development of cyber forensics and improved policies for managing cybercrime investigations.

In the partnership facilitated by the ISAC between industry and the law enforcement, it naturally empowers law enforcement in a decentralized manner. The flow of information from the companies will be controlled in a way that enables police to focus on investigations in aiding companies in identifying the identities of cyber criminals. And increase the ability of companies to cooperate with the prosecutors to file indictments against unidentified and identified criminal hackers. The law enforcement can also share information with the private sector by using ISACs as conduits. By communicating in a neutral forum that was created by the private sector industries, it is more likely to be accepted by the sector, and the sector will be more likely to share information. It will take time and regular meetings to build the relationships (executive and technical) between the law enforcement, ISAC, and member companies.

Relying on a neutral forum as a point of reference for both the private sector and the law enforcement will encourage both sides to come together to meet their common interests of combating cybercrime. As both groups learn to trust and cooperate with each other in their defined roles, the private sector companies can use the forum to communicate problems to the law enforcement and develop a cooperative solution in resolving issues. Ongoing security issue will vary among subgroups of the industries. ISACs can help prioritize the problems within the sub-groups and look for potential problems that affect the industry in a systemic manner. The law enforcement can either immediately resolve problems or create a plan to work towards an acceptable solution.

Performance assessments of the law enforcement and the ISAC determined by qualitative and non-qualitative categories in communication (especially in building relationships, identifying and resolving particular problems for the sub-groups within the industrial community); criminal investigations to identify criminal hackers; and arrests/extradition. While internal assessments conducted for the law enforcement organization's edification, there should also be a joint assessment conducted jointly with the other stakeholders- ISAC and the member companies. The joint assessment should be tied to performance-related pay and/or bonus. The appraisal would be on an annual basis and evaluations provided by not just the law enforcement but also other stakeholders in the three-way partnership between the private sector and the law enforcement. This scenari maintains an environment of transparency and cooperation between the three parties.

The application of community policing in cyberspace by the United States can be a leading example of innovation on fighting cybercrime against companies. The global implications of applying a decentralized policing strategy will encourage other national governments to model a functioning public-private partnership that coordinates efforts between the law enforcement and the private sector companies in mitigating and responding to cybercrimes. The borderless nature of cyberspace does not allow a purely one-sided solution either from the users or the government. The former group does not have the legal standing to enforce laws and the latter does not have the technology or the human capital to enforce laws effectively. The community policing solution will not solve all of the possible types of cybercrimes committed within cyberspace, but it is a start to a decentralized and yet systematic response in the aftermath of cybercrimes against industries. The decentralized approach will enable both law enforcement to respond more effectively by investigating cybercrimes and efficiently communicating with companies on evolving real-time threats. Real life policing will not mitigate all forms of cybercrime because the complications posed by the asymmetrical environment. Defenders invest further into its network security more than attackers have to invest into coding. While this proposal aims to improve policing on its own, it does not address other issues vital to establishing a sustainable global system to improve the overall security within cyberspace. Other components to improve prosecution will involve improving extradition and prosecution. Successful arrests of criminal hacker and prosecution will improve attribution and increase the risk that criminals must consider before committing cybercrimes.

### Challenges to the Adoption of 'Community Policing'

There are a number of significant challenges to the adoption of the concept but in a controlled environment with a small number of stakeholders make the concept feasible. Some of the challenges are technical, but the most significant obstacle will stem from the leadership of both public and private sectors. This kind of investment will require the significant political will to enact from both parties. Additional complications will include funding, opposition from entrenched agencies with overlapping missions, and inertia to deviate from the status quo. Companies and the government organizations are likely to be resistant to funding new concepts unless there is an obvious benefit or measurable returns. There are other cybersecurity tactics and third party cybersecurity firms that are also competing for attention and more importantly funding. While the concerns are valid about experimenting with new concepts. It is worthwhile to note that the technical portion of the concept can be established with a small group of similar portfolio companies and ISAC technical staff in conjuncture with FBI cyber forensic experts and law enforcement officers. This concept can gradually expand to other industries and their respective ISACs.

To change the current status quo will require leaders to have enough courage to move their organizations beyond inertia in regards to cybercrimes and cybersecurity. The biggest challenge will be to persuade the leadership of both sectors to participate. They are likely to be skeptical of the community policing because the concept has not be proven to work. Oakland is an example of a city that attempted to implement community policing strategy in its policing. It provided mixed results but its lack of success was due to the insufficient investment in placing officers within communities on a long term basis. There was insufficient time to build the necessary relationships and trust to create an environment to openly communicate.[52] Officers that were able to build relationships with the community improved the sense of security and cooperation from community members to lowered crime rates within the neighborhood.[53] Results from the real world implementation of community policing need to be analyzed for its return on investment by leadership. The program shows potential, but it needs sufficient investment in order for potential to be realized.

There is also the technical challenge of securely transmitting information to the ISAC for establishing a normal range of activity and continuous monitoring of abnormal activity. It may appear to be a challenge but many companies already contract its security through existing cybersecurity firms. ISAC will have to reassure companies that it will not inadvertently reveal confidential business information to other member companies.

The law enforcement lacks a coherent strategy in how cyber incidents are investigated and how the work should be divided between government agencies. The FBI

[52] Furloni, Mario, and Thomas Gorman. "After Five Years of Measure Y, Oakland Asks "Is Community Policing the Answer?"" Oakland North. January 21, 2010. Accessed February 6, 2015. https://oaklandnorth.net/2010/01/21/after-five-years-of-measure-y-oakland-asks-“is-community-policing-the-answer”/.

[53] Ibid.

is currently the leading agency in charge of policing cybercrimes affecting all US-based victims and the Secret Service in charge of financial related cybercrimes. These two law enforcement agencies do not have enough agents to investigate all of the cybercrimes affecting the private sector. The pooling of activity will allow officers the ability to focus on portfolios of companies and also to create a relationship with the group.

Even with the successful adoption of the 'community policing' practice, there is a lack of professionals experienced in the technical and legal areas dealing with cybercrimes. ISACs will have to hire a significant number of technical cybersecurity professionals experienced in continuous monitoring, analysis, and evidence processing.

**Policy Recommendations**

In order to implement the concept of 'community policing', this paper recommends that the one of the larger ISACs specifically the financial services industry as the first industry to experiment with the concept. The Financial Services-Information Sharing and Analysis Center is the appropriate organization to conduct third party analysis of cyber-related activity and act as a conduit to facilitate communication between companies and the FBI, Secret Service, and other agencies in cybercriminal investigations. It has a large membership base with 4400 member institutions which allows the organization to develop a smaller group of similar firms to participate in implementing the concept.[54] All of the involved organizations will be able to further the development of cyber analysis, forensics, evidence processing and storage, and prosecution of these criminals. The funding for the project should be jointly funded by FIN-ISAC and Department of Homeland Security as an attempt to fulfill EO 13636.

[54] "Global Perspective." FS-ISAC : Financial Services. https://www.fsisac.com/global-perspective (accessed January 17, 2014).

The ISAC is currently organized for tiered access with annual membership dues. The organization will need to recruit more company members in order to capture enough data. In order to increase involvement from larger companies, the Securities Exchange Commission need to require publically traded companies to report cyber-related incidents. Industry regulators such as Financial Industry Regulatory Authority (FINRA) can encourage companies that are interested in improving cybersecurity, to participate in the ISAC. As the SEC further defines and enforce the requirement that public companies report cyber-related incidents, it will increase participation from the large companies to engage on a proactive basis. The publicity of involvement from large companies will generate interest and involvement from SMEs.

The leadership from the top will have to become more educated in cybersecurity in cyberspace. The knowledge will prepare them to manage the complexities of managing security from an organizational standpoint. The education will prepare them to answer questions from investors and government officials that are inquiring about the organization’s strategy for security. If there needs to be an incentive for leadership to participate, organizations do not have to look further than Target’s mismanagement of a major breach of its payment network. The CEO of Target resigned after much criticism of its mismanagement of the response and recovery stemming from the breach.

Currently, there is already a significant gap in skilled professionals in the technical area of these. Law enforcement agencies and prosecutors will need to have additional training to understand the technical aspects of cybercrimes and encouraged to develop formal policies and procedures in response to the new operating field. The National Computer Forensics Institute (affiliated with the Secret Service) would train federal officers and prosecutors about the challenges of dealing with cybercrimes and provide them with tools to overcome them.[55]

There will also need to be an open and secure line of communication with companies and law enforcement to share information. A dedicated database would be used to store data such as a baseline activity and evidence gathered from attacks. Cyber forensics would analyze the evidence and share the findings with law enforcement. The partnerships would share evidence with law enforcement and other national security agencies for investigations.

The ways crimes are committed are ever changing but not the intent. To catch up to criminals, agents have to be fluent in the same spaces where the criminals operate. Law enforcement will need to show that it will prioritize the needs of the communities rather than its own. A first step in focusing on building the important relationships to improving perception and reality of improving policing would be hiring agents dedicated to training and investigating these types of crimes.

## Conclusion

The exponential growth of an innately fluid cyberspace has also increased the complexity of which companies have to navigate while conducting business. The constant change within cyberspace has created as many obstacles as opportunities for leadership of both private and public sectors. Current policing has not shown that terrestrial policing can be applied to cyberspace due the inability for law enforcement to police beyond physical territories. Attempts to bring global order into cyberspace have not been successful due to the lack of widespread adoption of treaties focused on

[55] White Vance, Joyce. "Forensics: Secret Service Computer Forensics Training Facility." U.S. Department of Justice: United States Attorneys on Cybercrime. http://www.justice.gov/usao/briefing_room/cc/forensics.html (accessed January 17, 2014).

cyberspace.

Cybercrime can no longer be considered a threat that can be effectivel managed on an individual basis, especially for SMEs. SMEs face an outsized investment in individually managing the risk. It is a systemic risk that needs systemic management by empowering companies to manage the risk in a coherent manner.  Significant improvements in policing within cyberspace will help bring some reassurances to businesses particularly the numerous SMEs that dominate the real world business landscape. Harnessing the power of an entire industry will empower the industry to work together to improve the overall security while operating in cyberspace.

By applying the concept of 'community policing' in cyberspace and  separating the needs of user groups and focusing on sub user groups such as SMEs, the focus will highligh the weaknesses and abilities of the sub-user group such as SMEs. SMEs individually are not particularly well equipped to deal with systemic threats of cybercrimes. But power of broad industry participation helps increase the awareness of systemic threats in cyberspace and the sharing of best practices tailored for companies by size and industry subgroup. Large and SMEs will benefit from sharing information and hiring third party analysis of unusual cyber activity. It will help law enforcement to focus on identifying and arresting suspected criminal hackers and then use the evidence gathered by the industry public-private partnership. The concept is not applicable to all problems stemming from cybercrimes but it does help further the development of cyberspace policing to improve attribution and aid in prosecution of suspected criminal hackers.

The application of "community policing" in cyberspace is a step towards improving policing in cyberspace for businesses and the government. It is a simple approach towards one of the many aspects of combatting cybercrime but something easy for leaders and the public to understand and participate. Since the concept is arguably abiding by the EO 13636, it should get partial funding from the Department of Homeland Security. This concept that is technology agnostic and voluntary. It provides a secondary but still very active monitoring for companies of all sizes. The initial funding will be a sign of confidence in implementing new concepts for policing cyberspace and protecting the US' private sector infrastructure.

The most important aspect of the community policing is the communication and coordination between the leaders of private sectors and the law enforcement. It will be the foundation for fostering a productive partnership to respond to serious incidents, quickly and efficiently as possible. It also can offer streamlined responses by allowing the ISACs coordinate the communication of cyber-related incidents to the appropriate law enforcement agency.

Improvement in security for industries will lead the way to other innovation such as securing cyberspace for all user groups. Utilizing the existing resources of industry and the federal government will provide a strong foundation for innovation in policing the borderless cyberspace. It will take time to make it possible for a secured cyberspace but taking small steps like these will help build trust and encourage additional cooperation. Improved security in cyberspace is good for business and government.

## Bibliography

"2012 Cost of Cyber Crime Study: United States." Ponemon Institute. www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf (accessed July 31, 2013).

"2012 Internet Crime Report." Internet Crime Complaint Center. www.ic3.gov/media/annualreport/2012_IC3Report.pdf (accessed May 20, 2013).

"APT1-Exposing One of Chinese's Cyber Espionage Units." Mandiant. intelreport.mandiant.com/Mandiant_APT1_Report.pdf (accessed June 12, 2013).

"About FS-ISAC." Financial Services- Information Sharing and Analysis Center. https://www.fsisac.com/about (accessed September 14, 2013).

"About FS-ISAC." FS-ISAC : Financial Services. https://www.fsisac.com/about (accessed December 7, 2013).

"Advanced Persistent Threats: How They Work | Symantec." Symantec. http://www.symantec.com/theme.jsp?themeid=apt-infographic-1 (accessed June 10, 2013).

Brennan, John. "Cybersecurity Awareness Month Part III | The White House." The White House. http://www.whitehouse.gov/blog/Cybersecurity-Awareness-Month-Part-III (accessed June 19, 2013).

"Build software better, together.." GitHub. https://github.com/ (accessed January 9, 2014).

"CSIS: 20 Critical Security Controls: Version 4.0." SANS Information, Network, Computer Security Training, Research, Resources. http://www.sans.org/critical-security-controls/guidelines.php (accessed June 19, 2013).

"Captive Insurance Companies." National Association of Insurance Commissioners. http://www.naic.org/cipr_topics/topic_captives.htm (accessed February 18, 2014).

Chabinsky, Steven. "Statement Before the Senate Judiciary Committee, Subcommittee on Terrorism and Homeland Security Washington, D.C.." FBI. http://www.fbi.gov/news/testimony/preventing-terrorist-attacks-and-protecting-privacy-rights-in-cyberspace (accessed March 24, 2014).

Claburn, Thomas. "Record-Setting Data Breach Highlights Corporate Security Risks." InformationWeek. http://www.informationweek.com/security/vulnerabilities-and-threats/record-setting-data-breach-highlights-corporate-security-risks/d/d-id/1110930? (accessed March 22, 2014).

Collins, Chris . "Opening Statement of Chairman Chris Collins- Protecting Small Businesses Against Emerging and Complex Cyber-Attacks." Subcommittee on Health and Technology. smallbusiness.house.gov/uploadedfiles/3-21-13_chris_collins_opening_statement.pdf (accessed September 8, 2013).

Constantin, Lucian . "Microsoft: Almost 90 percent of Citadel botnets in the world disrupted in June." PCWorld. http://www.pcworld.com/article/2045282/microsoft-almost-90-percent-of-citadel-botnets-in-the-world-disrupted-in-june.html (accessed December 21, 2013).

White House. "Critical Infrastructure Protection (PDD 63)." Federation of American Scientists. http://www.fas.org/irp/offdocs/pdd/pdd-63.htm (accessed August 29, 2013).

"Cyber Security." Lockheed Martin. http://www.lockheedmartin.com/us/what-we-do/information-technology/cyber-security.html (accessed June 18, 2013).

"Cyber Solutions." Lockheed Martin. http://www.lockheedmartin.com/us/products/cyber-solutions.html (accessed June 18, 2013).

"ETS No. 185 - Convention on Cybercrime." Council of Europe - Treaty Office. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (accessed August 6, 2013).

"Electronic Crimes Task Forces and Working Groups." United States Secret Service. http://www.secretservice.gov/ectf.shtml (accessed August 6, 2013).

Finkle, Jim. "Exclusive: Microsoft, FBI take aim at global cyber crime ring." Reuters. http://www.reuters.com/article/2013/06/05/net-us-citadel-botnet-idUSBRE9541KO20130605 (accessed December 21, 2013).

Finklea, Kristin M. , and Catherine A.  Theohary . "Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement." Federation of American Scientists. http://www.fas.org/sgp/crs/misc/R42547.pdf (accessed December 9, 2013).

Fisher, Dennis . "What is a Botnet? -Kaspersky Daily | We use words to save the world | Kaspersky Lab Official Blog." Kaspersky Lab Daily. http://blog.kaspersky.com/botnet/ (accessed December 21, 2013).

"Global Perspective." FS-ISAC : Financial Services. https://www.fsisac.com/global-perspective (accessed January 17, 2014).

Goossens, Ehren. "AMSC Surges After U.S. Charges Sinovel With Theft of Code - Bloomberg." Bloomberg . http://www.bloomberg.com/news/2013-06-28/amsc-surges-after-u-s-charges-sinovel-with-theft-of-code.html (accessed September 7, 2013).

Greenwald, Judy. "Target has $100M of cyber insurance, $65M of D&O cover: Sources." Business Insurance.

https://www.businessinsurance.com/article/20140114/NEWS07/140119934?tags=%7C306%7C338%7C299%7C329%7C75%7C76%7C302%7C303 (accessed January 29, 2014).

Manhattan Institute. "How New York Became Safe: The Full Story by George L. Kelling, City Journal 17 July 2009." City Journal. http://www.city-journal.org/2009/nytom_ny-crime-decline.html (accessed December 29, 2013).

Hutchins, Eric, Michael Cloppert, and Rohan Amin. "Intelligence-Driven Computer Network Defense." Lockheed Martin. www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf (accessed June 17, 2013).

"Information Sharing: A Vital Resource for a Shared National Mission to Protect Critical Infrastructure." Homeland Security. http://www.dhs.gov/information-sharing-vital-resource-shared-national-mission-protect-critical-infrastructure (accessed December 7, 2013).

Lewis, James. "Raising the Bar for Cybersecurity." Center for Strategic and International Studies. csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf (accessed June 17, 2013).

Menn, Joseph . "Major Companies Keeping Cyber Attacks Secret from SEC, Investors: Report." Insurance Journal News. http://www.insurancejournal.com/news/national/2012/02/02/233863.htm (accessed December 4, 2013).

"Michael Daniel." The White House. http://www.whitehouse.gov/blog/author/Michael%20Daniel (accessed May 19, 2013).

Obama, Barack . "Executive Order 13636â€"Improving Critical Infrastructure Cybersecurity ." Government Printing Office. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf (accessed January 16, 2014).

"Organiser of Darkmarket fraud website jailed." BBC News . http://news.bbc.co.uk/2/hi/uk_news/8539680.stm (accessed August 6, 2013).

Parrish, Karen. "Lynn: Cyber Strategyâ€™s Thrust is Defensive." United States Department of Defense (defense.gov). http://www.defense.gov/news/newsarticle.aspx?id=64682 (accessed June 13, 2013).

"Part 1: On the Front Lines with Shawn Henry." FBI. http://www.fbi.gov/news/stories/2012/march/shawn-henry_032712/shawn-henry_032712 (accessed December 11, 2013).

Pasquali, Valentina. "The Untold Cost of Cybersecurity." Global Finance. www.gfmag.com/archives/175-may-2013/12482-cover-growing-threat-the-untold-costs-of-cybersecurity.html#axzz2esYdwWKl (accessed September 14, 2013).

Riley, Michael, and Ashlee Vance. "China Corporate Espionage Boom Knocks Wind Out of U.S. Companies - Bloomberg." Bloomberg. http://www.bloomberg.com/news/2012-03-15/china-corporate-espionage-boom-knocks-wind-out-of-u-s-companies.html (accessed August 3, 2013).

Runde, Daniel F. , Holly Weiss, Anna Saito Carson, and Eleanor Coates. "Seizing the Opportunity in Public-Private Partnerships." CSIS. http://csis.org/files/publication/111102_Runde_PublicPrivatePartnerships_Web.pdf (accessed March 26, 2014).

"SQL Injection." US-CERT. http://www.us-cert.gov/security-publications/sql-injection (accessed March 26, 2014).

"Second Annual Cost of Cyber Crime Study." HP. www.hpenterprisesecurity.com/collateral/report/2011_Cost_of_Cyber_Crime_Study_August.pdf (accessed June 9, 2013).

US CERT. "Security Tip (ST04-015)." Understanding Denial-of-Service Attacks. http://www.us-cert.gov/ncas/tips/ST04-015 (accessed March 24, 2014).

"Summary of the Convention on Cybercrime (CETS No. 185)." Council of Europe - Treaty Office. http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm (accessed August 4, 2013).

"Treaty Office." Council of Europe . http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (accessed July 24, 2013).

"U.S. Strategic Command - U.S. Cyber Command." U.S. Strategic Command - Home. http://www.stratcom.mil/factsheets/Cyber_Command/ (accessed May 18, 2013).

"USDOJ: Five Indicted in New Jersey for Largest KnownData Breach Conspiracy." United States Department of Justice. http://www.justice.gov/opa/pr/2013/July/13-crm-842.html (accessed September 15, 2013).

"Vision and Mission Statements." United States Secret Service. http://www.secretservice.gov/mission.shtml (accessed August 4, 2013).

"Welcome to the Domestic Security Alliance Council." Domestic Security Alliance Council. http://www.dsac.gov/Pages/index.aspx (accessed December 21, 2013).

"What Is Critical Infrastructure?." Homeland Security. http://www.dhs.gov/what-critical-infrastructure (accessed December 7, 2013).

White Vance, Joyce. "Forensics: Secret Service Computer Forensics Training Facility." U.S. Department of Justice: United States Attorneys on Cybercrime. http://www.justice.gov/usao/briefing_room/cc/forensics.html (accessed January 17, 2014).

Wilshusen, Gregory C.. "CYBERSECURITY- Threats Impacting the Nation." Government Accountability Office. www.gao.gov/assets/600/590367.pdf (accessed June 17, 2013).

Yadron, Danny, Paul Ziobro, and Devlin Barrett. "Target Warned of Vulnerabilities Before Data Breach." The Wall Street Journal. http://online.wsj.com/news/articles/SB10001424052702304703804579381520736715690 (accessed February 16, 2014).

Zetter, Kim. "Document Reveals TJX Hacker's Assistance to Prosecutors | Threat Level | Wired.com." wired.com . http://www.wired.com/threatlevel/2009/12/gonzalez-memo/ (accessed September 15, 2013).

## Captive Insurance: Providing Cybersecurity Risk Transfer for SMEs

### Introduction

The recent rise of data breaches in large publicly traded companies such as T.J. Maxx, Neiman Marcus, and Target have shown that companies are encountering cyber breaches, despite effort to mitigate such risk.[56] Companies managing the recovery from such incidents require a good deal of resources in order to respond sufficiently to such events. Target one example of a large business that experienced hacking through its point of sale machines. The breach through the underbelly of Target's technology broke the trust of consumers and severely damaged the brand reputation. Target re-issued a quarterly estimate with a decline of 2.5% in sales compared to flat comparable sales before the hacking occurred. [57] The company issued a statement that it planned to make an investment of $100 million in security upgrades to its payment system.[58] Finally, the CEO and Chairman of Target resigned over the poor management of the situation.[59] The consequences that Target experienced in the aftermath of a serious hacking event despite the prior assumptions of compliance shows that planning for such events is vital. Consumers, investors, and governments expect companies to have a thorough recovery plan for cyber incidents of kinds.

[56] Schectman, Mark. "When to Disclose A Data Breach: How About Never?." Wall Street Journal. http://blogs.wsj.com/riskandcompliance/2014/03/27/when-to-disclose-a-data-breach-how-about-never/ (accessed April 2, 2014).

[57] Mcgrath, Maggie. "Target Data Breach Spilled Info On As Many As 70 Million Customers." Forbes. January 10, 2014. Accessed December 27, 2014. http://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/.

[58] Pagliery, Jose. "Target Exec Gives Hack Details to Senate." CNNMoney. February 14, 2014. Accessed December 27, 2014. http://money.cnn.com/2014/02/04/technology/security/target-senate/.

[59] O'Connor, Clare. "Target CEO Gregg Steinhafel Resigns In Data Breach Fallout." Forbes. May 5, 2014. Accessed December 27, 2014. http://www.forbes.com/sites/clareoconnor/2014/05/05/target-ceo-gregg-steinhafel-resigns-in-wake-of-data-breach-fallout/.

The largest US companies are more likely to have established policies, resources, and people to respond such incidents. But the majority of the companies operating in the US are small and medium enterprises and not all of those companies have the proportional access to such resources.[60] There is concern whether SMEs can cope with the costs of recovering from cyber incidents because it has fewer resources. Target experienced an event that influenced its earnings for the quarter and beyond, but it is still in business due to its substantial balance sheet; SMEs do not share that kind of luxury. The economic loss caused by business interruption in cyberspace or a malicious incident can be detrimental to any company; a large company will be able to absorb the costs compared to a SME because it will likely have a greater proportional effect on a SME's balance sheet.

While companies may have access to disparate resources for cyber incidents, there is still no assurance that the company has taken sufficient actions to assess its weaknesses fully and implemented necessary mitigation for managing cyber risk and comprehensive plan to respond to emergencies. Insurance is one of the most useful tools to ensure minimal risk management through underwriting requirements and audits of losses incurred by insured companies.[61] Insurance is a tool used by companies to transfer a portion of the risk of operating in cyberspace. It provides financial compensation for the insured company to recover some of the economic loss triggered by an incident and funds for the company to use for recovery in the aftermath of cyber incidents, malicious or not. Depending on the type of insurance it will provide coverage for first and/or third party

[60] "Statistics about Business Size (including Small Business)from the U.S. Census Bureau." US Census Bureau . https://www.census.gov/econ/smallbus.html (accessed April 1, 2014).

[61] Kirilov, Rosen. "Effectiveness of the Information Security in the Banks."Cybernetics and Information Technologies 6, no. 2 (2006).

losses. In order to obtain such insurance, companies must complete specific requirements in order to qualify for underwriting. Insurance companies will provide guidance on expected policies and practices to mitigate as much risk as possible in order for the insurance company to accept the unknown risks of the insured company operating in cyberspace.

Traditional insurance coverage is increasingly excluding coverage for cyber- related risks.[62] The assumption, for most companies, is that traditional insurance will provide coverage for those same risks insured for the real world will carry over to cyberspace. That is not the case with cyber risks; more insurance companies are explicitly excluding cyber/electronic losses in the detailed portion of the insurance policy. The risk has been deemed to be substantially different from the currently available actuarial information on non-cyber losses.[63] Large companies have or will be increasing investments in specific cyber- insurance, while SMEs are mostly either relying on current insurance such as professional liability (errors & omissions) or general liability insurance to provide coverage for cyber-related risks and losses. SMEs that assume existing insurance coverage will provide financial compensation for cyber incidents can be an expensive mistake. A company that inadvertently invests further in existing insurance without expert knowledge that the insurance policy will cover the appropriate risks can further reduce the return on investment in the insurance as well reduce the resources spent on recovery.

Cyber insurance is a burgeoning category within the insurance industry.  It is specially designed to provide coverage for direct and indirect, non-tangible losses such as

[62] Jackson, William D., Mark Jickling, and Baird Webel. "The economic impact of cyber-attacks." Congressional Research Service, Library of Congress, 2004.

[63] Majuca, Ruperto P., William Yurcik, and Jay P. Kesan. "The evolution of cyberinsurance." arXiv preprint cs/0601020 (2006).

confidential data (personal identification information and financial information), electronic network technology (i.e. cloud computing), and electronic business interruption (caused either by technical error or malicious cyber-crime.) Current commercial insurance coverage for cyber-related risks is limited, and custom cyber insurance policies are expensive.[64] Large enterprises typically have purchased large amounts of commercial cyber insurance in addition to tailored insurance, but SMEs do not normally purchase it.[65] The significant growth in the cyber insurance market is increasing the availability of such products to participants, but there are potential issues for companies, especially SMEs.

There are risks to SMEs considering participation in a developing cyber insurance market. As insurers receive more premiums, they will also process more claims filed by the insured companies. One of the risks with the additional claims filed is the insurance company may not find that it is profitable to provide such a service or reject the claim outright. Any company that files a claim, especially SMEs, will want an expeditious claims process and access to re-insurance will need to consider alternatives to commercial cyber insurance. One of the lesser-known alternative that can be used by SMEs to create cyber coverage without traditional commercial insurance is through the creation of captive insurance companies. Captive insurance is an insurance company soley created to insure the parent company or companies. Traditionally this has been utilized by large enterprises that had to insure multiple subsidiary business units but did not offer any other apparent benefits that would incentivize SMEs to participate. This paper asks if captive insurance is a viable solution for SMEs to transfer risk in the

[64] Brockett, Patrick L., Linda L. Golden, and Whitley Wolman. "Enterprise Cyber Risk Management." Risk management for the future–Theory and cases (2012).
[65] Ibid.

immediate future while general commercial cyber insurance market continues its development.

SMEs function under a number of constraints in comparison to large enterprises, while considering cyber insurance coverage. The paper will review major constraints that fall under these main themes: budget, human capital, and policies. The understanding of captive insurance companies as a viable solution is an examination relative to the current state of the insurance market.

This paper consists of six parts. The first part will introduce the literature review and essential definitions to understand cyber insurance. The second part of the paper will provide an overview of existing role and state of cyber insurance in overall risk management for companies operating in cyberspace. The third part of the paper will review the roadblocks to developing a mature commercial cyber insurance market. Then this paper will examine captive insurance as an alternative to the commercial cyber insurance. The fifth part of the paper will explore three examples of companies and their respective experiences in managing the cyber-related incident and the role of insurance played in each case. In the conclusion, the paper will examine the analysis of the three case studies and the importance of risk management for SMEs.

## Literature Review

This paper examines whether a captive insurance company is a viable solution for the immediate future for SMEs. It looks for a solution in the immediate future rather than in the future because the market will become more efficient over time. Insurance companies will eventually have access to greater quantities of data related to cyber incidents that will help calculate accurate pricing for the risk that insurance companies will accept from an insured company. Access to improved actuarial data and increased demand for this cyber insurance will help further the development of the market. Premium prices for cyber insurance will eventually become more efficient but there are no guarantees on the direction of the market as of yet.

*Definitions for Traditional Commercial Insurance*

First party business insurance policies provide financial compensation for direct losses or damages to the insured's property and may provide coverage for lost business revenue.[66] The insurance applied in a non-cyber context will provide monetary compensation for damages to inventory, vital machinery, and factories because of either vandalism, theft, destruction from a natural disaster or inoperability.

General business liability insurance covers third party losses/injuries occurred on the insured company's assets and property.[67] These would be losses incurred neither by the insured company nor the insurance company. The insurance will provide compensatory damages, nonmonetary losses suffered by the injured party, and punitive damages.

Errors and omissions (E&O) insurance provides coverage for the failure to provide or service provided, to meet the client's expected results or promised results.[68] It will cover judgments, settlements, and defense costs. This type of insurance may or may not include loss of client data, software or system failure, claims of non-performance. It will not include it because electronic losses are considered to be intangible.

[66] Paar, Randy, Elizabeth Sherwin, David Elkind, and Kirk Pasich. "A Policyholder's Primer on Insurance." Dickstein Shapiro. http://www.dicksteinshapiro.com/files/upload/Insurance_Coverage_Primer_A_Policyholder's_Primer_on_Insurance.pdf (accessed March 31, 2014).

[67] "Commercial General Liability Insurance." Texas Department of Insurance. http://www.tdi.texas.gov/pubs/pc/pcgenliab.html (accessed March 30, 2014).

[68] Wertz, Glenda. "The Ins and Outs of Errors and Omissions Insurance." Insurance Journal News. http://www.insurancejournal.com/magazines/features/2004/07/19/44745.htm (accessed March 31, 2014).

Director and Officers Liability- is coverage for directors and executives liability while serving the policyholder company in a fiduciary capacity.[69] It is very similar to E&O insurance, but it is tailored more for the management of a company rather than just professionals. This type of insurance will typically include legal expenses and settlements for lawsuits brought against executives and companies.

The prior definitions for traditional commercial insurance provide coverage for a variety of items, but none have explicitly included electronic data, electronic/virtual systems, losses due to unexpected disruptions in electronic systems. While it can be argued that it should cover liability in cyberspace, the lack of explicit inclusion has allowed insurance companies to deny claims filed by insured companies. Lawsuits initiated by policyholders against insurance companies have not been successful such as the case of Zurich America and Zurich Insurance versus Sony in its 2011 highly publicized data breach of its PlayStation Network.[70] The insurers were able to absolve themselves of providing financial compensation to Sony because the general liability insurance did not explicitly include third party theft of personal information.

## Cyber Insurance as a Risk Management Tool

There are typically four approaches in risk management while treating known risks- avoidance, mitigation, transfer, and acceptance.[71] Some have argued that finding an optimal risk management strategy should focus on the economically optimal solution rather than the potential technical loss that leads to greater understanding from business

[69] "How to Determine Whether to Insure Directors and Officers BY Inc. staff." Inc.com. http://www.inc.com/guides/2010/12/how-to-determine-whether-to-insure-directors-and-officers.html (accessed March 31, 2014).

[70] Shrestha, Bibeka . "Details Emerge On Ruling Nixing Sony's Cyber Coverage." Law360. http://www.law360.com/articles/515200/details-emerge-on-ruling-nixing-sony-s-cyber-coverage (accessed April 2, 2014).

[71] Stoneburner, Gary, Alice Goguen, and Alexis Feringa. "Risk management guide for information technology systems." Nist special publication 800, no. 30 (2002): 800-30.

leaders.[72] Determining the optimal solution requires the application of certain standards such as NIST (National Institute of Standards and Technology) or ISAME (Information Assurance for SMEs) in order to scrutinize the information security systems and its risks without the intense investment as ISO 27001.[73] Such assessments will provide a vital starting point for SMEs to be aware of the capabilities of existing security systems and areas of improvement to mitigate risk. Policies and procedures for operating in cyberspace will mitigate some of the risks. Companies will then create contingency plans that will include incident response plans, disaster recovery plan, and business continuity plan that will address potential events that include cyber-related incidents.[74] Companies operating in cyberspace have already accepted some form of risk. Obviously the risk accepted is less than the benefits derived from operating in cyberspace. Those companies that wish to avoid the risk of operating in cyberspace may not be active participants but will encounter third party risk by interacting with other stakeholders who are operating in cyberspace.[75] Finally, some companies willing and able to transfer cyber risk to an insurance company. [76] The necessary insurance can be decided after modeling the probability of certain scenarios and potential losses. While direct losses would be obvious, for SMEs, business leaders would have to devise a way of calculating indirect losses associated with the risks identified with their business.

[72] Anderson, Ross. "Why information security is hard-an economic perspective." InComputer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual, pp. 358-365. IEEE, 2001.
[73] Henson, Richard, Daniel Dresner, and David Booth. "IASME: Information Security Management Evolution for SMEs." (2011): 1-11.
[74] Carneiro, Alberto. "Adopting new technologies." Handbook of business strategy7, no. 1 (2006): 307-312.
[75] Bojanc, Rok, and Borka Jerman-Blažič. "An economic modelling approach to information security risk management." International Journal of Information Management 28, no. 5 (2008): 413-422.
[76] Bolot, Jean, and Marc Lelarge. "Cyber Insurance as an Incentivefor Internet Security." In Managing information risk and the economics of security, pp. 269-290. Springer US, 2009.

Risk avoidance and risk mitigation can appear to be the preferred tactics, but risk transfer can benefit an organization's for managing unexpected, detrimental events that may not have previously established thorough planning. Insurance is effect tool in driving business leaders to engage in risk mitigation for all risks including cyber.[77] Some business leaders may not believe the investment in the insurance is necessary after the conducting the assessment. But the the exercise of examining whether insurance is necessary is beneficial for business leaders to gain a measured understanding of weaknesses within a framework of existing standards. Those that recognize that insurance is a necessity will create a mitigation plan and invest in insurance to cover the potential shortfall if the company experiences an event that causes losses.

### *Commercial Cyber Insurance*

Most companies lack proper risk management strategy much less cyber insurance. However, even those with sufficient traditional commercial insurance may find that existing policies with exclusions that would cover such incidents. Cyber insurance can be a useful tool to initiate the overall strategy in managing cyberspace risks for many SMEs. It will also force companies that did not previously formulate policies for securing confidential information, internal user policies, IT security including policies for securing personal mobile devices used for work, and data storage redundancy. It also gives the ability for companies to contemplate the role of technology in the business. The technology is now becoming agiler with storage in the cloud, and devices that benefit from the data interconnectedness more commonly known as the Internet of Things.[78] The

[77] Katz, David. "In the Trenches of the Cyber War." CFO. October 27, 2014. Accessed January 8, 2015. http://ww2.cfo.com/data-security/2014/10/trenches-cyber-war/.

[78] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54, no. 15 (2010): 2787-2805.

cost of the insurance premium will be dependent on the insurance company's willingness to accept a portion of the insured's unknown risk of liability in cyberspace. Companies will be intrinsically incentivized to invest in risk mitigation in order to lower the premium.[79] The insurance policy will also provide a way for the company to exchange uncertain costs of potential losses in the future for present costs. It helps control costs for budgeting of certain scenarios. Insurance provides cost control by the design of adoption and implementation of best practices.

The cyber insurance sub-industry currently has a number of distinct categories of coverage. It is unique because it provides explicit coverage that was previously not included in traditional commercial insurance. The loss covered will usually fall under direct and indirect losses similar to traditional insurance but the assets covered under cyber insurance will focus on electronic data, hardware, and cyber specific events. The coverage may include the loss and/or expenses related to business/service interruption, reinstatement of data and its security, electronic data assets managed by network technology, forensic services, litigation and settlement, and regulatory fines. This kind of insurance coverage is bridging an important gap within traditional insurance coverage for companies.

One of the emerging products within cyber insurance is cyber liability insurance. It can provide coverage for intangible losses from data breaches, denial of service, and interruption of service. It can provide financial compensation for technical services, forensics, notification, legal, regulatory, and administrative expenses related to incident

[79] Anderson, Ross, and Tyler Moore. "Information security: where computer science, economics and psychology meet." Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 367, no. 1898 (2009): 2717-2727.

response.[80] It is important because companies are required to report a breach to consumers, in 46 out of 50 states.[81] Depending on the insurance company offering this type of insurance, it may include coverage related to third-party supply chain risk and intellectual property.[82] This form of commercial insurance is still under development, but demand is growing for this type of product. While it is under development, there are also significant gaps in actuarial data to accurate price such form of risks. These deficiencies for cyber liability insurance are representative of the market itself.

Current commercial insurance policies for cybersecurity risks offer limited coverage while tailored commercial insurance policies are expensive for most companies. There are a few areas that insurance cover such as insurance to cover direct losses and liability for third party damages. Commercially available cyber insurance is either very expensive or limited coverage because of the lack of actuarial data or knowledge about the coverage. 17 carriers provide cybersecurity insurance policies today. Only five or six of those carriers are willing to develop “manuscripted” policies – custom-drafted from scratch.[83] While custom-drafted, it may include negotiations between the insured company and the insurance company to include certain coverage on riskier line such as direct losses. These policies tend to skew in favor of large enterprises with large budgets in order to afford highly customized insurance.

### *SMEs and Cyber Insurance*

[80] Cleveland, Bruce . "Cyber Liability Insurance — As a Cloud Provider Can You Afford Not To Have It?." Bruce Clevelands Rolling Thunder. http://www.interwest.com/rolling-thunder/on-demand/cyber-liability-insurance-as-a-cloud-provider-can-you-afford-not-to-have-it/ (accessed March 31, 2014).

[81] Sembhi, Sarb. "An Introduction to Cyber Liability Insurance Cover." An Introduction to Cyber Liability Insurance Cover. Accessed January 14, 2015. http://www.computerweekly.com/news/2240202703/An-introduction-to-cyber-liability-insurance-cover.

[82] Ibid.

[83] "Cybersecurity Insurance Workshop Readout Report." Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/cybersecurity-insurance-read-out-report.pdf (accessed April 1, 2014).

While companies should consider the inclusion of cyber insurance, there are some issues with demand from SMEs. There are several factors as to why most of SMEs lack proper cyber insurance. Many SME owners and employees do not have experience or working knowledge of technology or security required to maintain a secure working environment. In a National Cyber Security Alliance and Symantec survey of 1,015 SMEs (250 employees or less) in the United States, 11% of those surveyed said no one is responsible for cybersecurity at the business; 66% say the business owners/operators are responsible; 9% rely on an IT savvy employee and 8% use an outside IT consultant.[84] The lack of knowledgeable individuals in SMEs also will also often indicate a lack policies and tools such as insurance to respond to cyber incidents such as the Target case. 83% of the same respondents said that the company did not have formal Internet security policy. It is apparent the lack of involvement by executives will deprive interest in developing a coherent risk management strategy for unexpected cyber-incidents.

Most SMEs lack of budget to afford such product as the current cost of existing cyber insurance for first party losses. Most of the available cyber insurance for first party losses is expensive due to lack of actuarial data. First party losses are losses directly incurred by the insured. Finally, most SMEs assume that existing insurance will cover the company's cyber-related incidents when in reality it may not due to exclusions in traditional commercial insurance.

Despite the fact that such a large number of SMEs lack cyber insurance, they are also the group most at risk. Verizon reported in 2011 that 72% of 855 data breaches

[84] Ibid.

around the world targeted at companies with less than 100 employees.[85] It was a 62% rise in data breaches focused on SMEs from 2010. Small and medium sized enterprises (SME) are vulnerable to data breaches and other internal and external cybersecurity risks such as network disruption, insider threat, denial of service attacks, physical damage or loss of data, or malware, or corporate espionage. The lack of knowledgeable individuals to manage the risk of operating in cyberspace can lead to a lack of awareness of the necessary tools to protect itself. Many SMEs will utilize generic security tools that are vulnerable to exploitation if the hacker has already uncovered them. Depending on the cost of the incident response plus the intrinsic value of the data that was affected, a cyber-incident can be devastating for a SME. The consequences of these risks can lead to a disruption in operations, failure to fulfill contractual obligations, and loss of third party information.

### Commercial Cyber Insurance Insufficient for SMEs

Cyber insurance is a growing and popular sub-sector with within the industry. The insurance industry as a whole is not known to be dynamic. Insurance designed for mass use was carefully calculated to anticipate the amount of acceptable losses as understood under the law of large numbers. It is one that is naturally conservative in its development of products that will accept unexpected but quantifiable risk from others. There is interest in developing products to provide a variety of coverage for cyber-related incidents. However, there are also barriers to creating a comprehensive availability of commercial insurance such a lack of a third party market to cover losses that are associated to cyber-related incidents.

[85] Baker, Wade, A. Hutton, C. David Hylender, J. Pamula, C. Porter, and M. Spitler. "2011 data breach investigations report." Verizon RISK Team, Available: www. verizonbusiness. com/resources/reports/rp_databreach-investigations-report-2011_en_xg. pdf (2011): 1-72.

There is an ongoing debate on the role of the government in managing cyber insurance risk. It is frequently compared to terrorism insurance because these are high-value catastrophic events for companies and government entities. Terrorism insurance faces the same issue of re-insurance. The Terrorism Insurance Act that provides the "backstop" funding for commercial insurance requires extensions approved by Congress.[86] The Act has been extended by Congress in 2005, 2007, and 2015.[87] The most recent extension was only made after a few days of the prior legislation expired. It led to the expiration 750,000 private insurance policies after December 31, 2014 because the policies stated that the government had to provide the financial backstop to such policies.[88] While Congress eventually passed the renewal for such legislation, it highlights the fragile nature of the government willingness to provide such an important backstop. Some have made comparisons of cyber insurance to terrorism insurance with the proposal that the government provides a similar backstop to cyber insurance for major catastrophic events.[89] It reinforces the precarious nature of commercial insurance for companies because it policies explicit reliance on government reinsurance.

The actuarial information related to cyber insurance policies is under development. There is no standard access for such information since not all companies are legally required to report such incidents governmental entities. The current corporate culture does not encourage sharing. Public companies are now experiencing pressure to share information, but they are only starting disclose information due to regulatory rules.

[86] "TRIA Is Renewed, Finally..."The National Law Review. January 10, 2015. Accessed January 14, 2015. http://www.natlawreview.com/article/tria-renewed-finallyterrorism-risk-insurance-act.

[87] Ibid.

[88] Weisman, Jonathan. "Congress Passes Measure to Cover Terrorism Risk." The New York Times. January 8, 2015. Accessed January 14, 2015. http://www.nytimes.com/2015/01/09/business/renewal-of-federal-terrorism-insurance-clears-congress.html?_r=1.

[89] Orszag, Peter R. Homeland security and the private sector. Brookings Institution, 2003.

Privately held companies are not held to the same standards and are likely not to share information voluntarily due to a combination of legal, reputational, additional security risks, and financial risks.[90] The lack of such information makes it difficult accurately to price the risk associated with cyber risk. Insurance companies are forging ahead without such information while knowing that one catastrophic event may financially overwhelm the company before the market is developed.

These significant barriers on the supply side will take a long time to overcome as it did with other areas of insurance. While it will take time to create overcome these issues to provide accurately priced commercial cyber insurance to companies of all sizes, there is no doubt that demand will continue to grow. With more and more public companies are publically disclosing events and making significant investments in risk management, this will encourage SMEs to consider additional investment in security investments. While the demand from SMEs continues to develop for commercial cyber insurance, SMEs that need a solution that can solve the problem of risk transfer in the immediate future. SMEs that are reliant on number of suppliers and has significant amounts of sensitive data should consider cyber insurance but also insurance that is not at risk of overly relying on Congressional legislation and a quick claim process.

A novel option that has not been widely promoted to SMEs is captive insurance. Captive insurance is an insurance company established by a non-insurance parent company or group of companies to finance its individual risks.[91] It is a form of self-insurance against any number of risks associated to the insured. This tool has been used

[90] Jackson, William D., Mark Jickling, and Baird Webel. "The economic impact of cyber-attacks." Congressional Research Service, Library of Congress, 2004.

[91] "Captive Insurance Companies." National Association of Insurance Commissioners. http://www.naic.org/cipr_topics/topic_captives.htm (accessed February 18, 2014).

by many large corporations as one of its options to transfer risk. SMEs may not realize that they can also take advantage of the tool and receive a US tax benefit assuming its premium payments do not exceed IRS limits. There will be a considerable wait for the development of commercial cyber insurance for many SMEs while access to create an individual insurance company that will provide custom coverage specific to its needs including all applicable cybersecurity risks.

The adoption of captive insurance to provide custom cyber insurance coverage would be a stop-gap measure until there is a mature market to accurately price insurance and provide coverage that will not change due to legislation or inaccurate actuarial information. It is a tool that will attract attention from owners and executives in SMEs. It provides a variety of benefits of controlling the claims process, substantial tax benefits, and intrinsic incentive to improve cyber security within the firm.

Captive insurance is a closely held insurance company owned and controlled by the insured or various insured companies. It provides flexibility that insured companies that commercial insurance policies cannot provide. Creating a captive insurance company allows the insured company to determine its own loss requirements, make tax deductible premium payments to the captive insurance, access reinsurance market for cheaper premiums, and build its own separate budget for increased ability to address risk control.[92] Companies that are large enough can form its own insurance companies can remove the chance of moral hazard. Smaller companies will have to pool their risk together in mutual captive insurance. It may risk moral hazard, but the captive company will have to share the risk with a specific number of other captives if the captive wants

[92] Fox, Gary A., and Lynn M. McGuire. "Forming a Captive Insurance Company-Understanding the Business and Tax Implications." Tax Executive 64 (2012): 149.

the IRS approval. This concept of cyber insurance is in its early stages but for some it may be a feasible idea because of the ability for the insured company to have control over the risk transfer.

### *Captive Insurance Companies*

Captive insurance is an alternative form of insurance that is wholly owned and operated by the insured company or group of companies. There is a variety of captive insurance companies such as single-parent, group captive, association captive, rent-a-captive- and risk retention group.[93] This type of insurance company was traditionally utilized in times when commercial insurance was expensive and difficulty in obtaining certain types of desired insurance coverage. While the formation of a captive is a subsidiary to the insured, it is a legally formed company with a legitimate business plan to insure legitimate risks. The size of the captive insurance companies size is not restricted. While large holding companies tend to create captive insurance for its subsidiary companies, SMEs can also form its own captive insurance company. Small captives will have to have at least half of its premium pooled with other companies that share a similar risk. Zhao and Xue support the concept of captive insurance companies to streamline IT compliance management but while the authors support the arguments in favor of captive insurance, it does not offer clear reasons how SMEs would benefit from creating a captive insurance.[94] Schwarcz and Schwarcz point out the cumulative effect of insurance companies including captive insurance companies can create systemic risk.[95]

[93] Hall, Shanique. "Recent Developments in the Captive Insurance Industry." NAIC. http://www.naic.org/cipr_newsletter_archive/vol2_captive.htm (accessed March 30, 2014).
[94] Zhao, Xia, and Ling Xue. "A Framework of Using Captive Insurance to Streamline IT Control and Compliance Management." Journal of Information Privacy & Security 5, no. 3 (2009).
[95] Schwarcz, Daniel, and Steven L. Schwarcz. "Regulating Systemic Risk in Insurance." (2014).

There was not much scholarly research in the area directly related to captive insurance and cyber risk.

SMEs that wish to participate or form a captive insurance company can create a captive insurance company with additional tax benefits listed under Sec. 831(b.) Property and casualty insurance company that receives a gross premium income of $1.2 MM or less can elect that it can legally avoid tax on its premium income and only taxes on the income derived from the investment income.[96] The election for taxation only on the investment income is irrevocable without the IRS's consent, but it is automatically terminated if the gross premium income exceeds the section limit.[97] It allows the insured companies to reduce the amount of taxes by deducting the premium payment, and the captive insurance will be taxed on the investment income instead of the underwriting income received. For example, assuming a captive insurance company with the 831(b) designation received a premium of $500,000, and all of it is invested in a conservative investment yielding 4%. The captive insurance would be responsible for $20,000; the taxable amount of the investment income, compared to the typical amount of $500,000 of the premium received, that would have been identified as taxable without the special designation. Other insurance companies will have to pay taxes on the total premium received. It is a substantial tax benefit for companies that wish to control the risk transfer from the parent company.

The small captive insurance companies are also required to diversify the risk. The IRS Ruling 2002-89 stated that the captive insurance companies that receives 90% plus of premiums and if the parent company that owns over 90% of the captive insurance

[96] "26 U.S. Code § 831 - Tax on Insurance Companies Other than Life Insurance Companies." Legal Information Institute. Accessed January 21, 2015. http://www.law.cornell.edu/uscode/text/26/8

[97] Ibid.

company means that there has not been enough risk shifted from the parent company. The ruling further clarified that if the risk of the parent company was less than 50% of the captive insurance company's total risk and premiums received, that it would be a qualified tax deduction.[98] Further Ruling 2002-90 stated that domestic holding companies with 12 operating subsidiaries with similar but independent risks, if each subsidiary that has a minimum of 5% but no more than 15% of the total risk insured would also make insurance premiums paid a qualified tax deductions.[99] These two rulings were significant in clarifying the quantity of risk transfer from the captive insurance companies to re-insurance. In order to achieve the desired result of alternative taxation structure of the smaller captive and also making the insurance premiums deductible for the parent company.

There are a few other incentives that make captive an appealing option to SMEs currently interested in covering its cyber risks. The captive company can provide coverage on any legitimate risks that the insured parent company that is necessary. It can either provide primary or secondary coverage if the company already owns existing commercial insurance existing risks. The captive company can incentivize the insured parent company to implement better practices to mitigate risks including those while operating in cyberspace.[100] Its intrinsic incentive is that improved mitigation will lower the chances of processing claims and paying out funds. The captive insurance company can invest the premium paid into the company. The insurance company will have to pay

[98] Taylor, Greg, and Scott Sobel. "A Closer Look at Captive Insurance." The CPA Journal. June 1, 2008. Accessed January 31, 2015. http://www.nysscpa.org/cpajournal/2008/608/essentials/p48.htm.

[99] Ibid.

[100] Fox, Gary A., and Lynn M. McGuire. "Forming a Captive Insurance Company-Understanding the Business and Tax Implications." Tax Executive 64 (2012): 149.

taxes on any investment income earned, but it will be at a lower rate if the gains are counted as long-term capital gain. The premiums paid into the captive insurance company can also be used to purchase re-insurance. Re-insurance is insurance purchased by insurance companies to transfer risk to one or more insurance companies.[101] It allows additional diversification in the in the risk that has been transferred by insured companies to the insurance companies. Finally, the captive insurance company can provide an easier and expedited claim process.

Shetty, Schwartz, Felegyhazi, and Walrand argue that cyber insurance does not improve security.[102] This paper disagrees that insurance will not improve security. The captive insurance company can positively impact the bottom line of the parent company because net profits from the captive insurance company can return to the parent company. The parent company/insured is incentivized to not make claims. The way to not submit claims is to improve the security. To create a legitimate captive insurance requires that the captive insurance company adequately analyze and price the risk of the parent company. If the company does not take appropriate mitigation to have competitive pricing for its cyber risks, it may bring unwanted attention from the IRS for potential fraud.

## Case Studies

This paper will examine three companies in the context of cyber insurance in cyber-related incidents. Two of the case studies that presented are ones that involve major companies. While two of these cases involve well-known companies with substantial

[101] "Fundamentals of P/C Reinsurance." Reinsurance Association of America. http://www.reinsurance.org/Fundamentals/ (accessed March 30, 2014).

[102] Shetty, Nikhil, Galina Schwartz, Mark Felegyhazi, and Jean Walrand. "Competitive cyber-insurance and internet security." In Economics of Information Security and Privacy, pp. 229-247. Springer US, 2010.

resources, it will provide insight in how insurance is utilized after encountering cyber-related incidents. It will also provide some insight on how companies with proper and improper coverage can affect the outcome of resolving data breaches or other incidents. The third case study is one that involved a small private company that did not have any insurance that experienced an electronic theft from its bank accounts.

In 2011, Sony unexpectedly shut down Play Station and Qriocity in response to a major data breach. Malicious hackers accessed up more than 77 million records of user's account names, e-mail addresses, passwords, and credit card information.[103] Hackers also breached the other areas of Sony's Online Entertainment gaming website. Sony was notified of the intrusion on April 19th but did not send data breach notification emails to users until a week later. The Playstation Network had to be shut down and completely rebuilt. Sony's insurance companies that provided general liability insurance to the company immediately filed a claim in court. The insurance companies stated that it was not liable to provide legal defense for the third-party lawsuits from the users because the data breach because it was a third party breach not related to the insurance that was to be provided by the insurer. The class action lawsuits brought on by the users were based on Sony's inability to protect the information and the delay in notifying the users. Sony eventually dropped the lawsuit against Great American Insurance CO. of New York and lost approximately $25 million that it attempted to claim for the incident.

Sony experienced a very unfortunately event when it discovered that its commercial insurance had very strict qualifications for accepting claims, despite the size of the company. It lost significant money, double-fold because the money that was set

[103] Takahashi, Dean. "The cost of Sony's PlayStation Network outage: $24 billion or $20 million?." VentureBeat. http://venturebeat.com/2011/04/27/the-cost-of-sonys-playstation-network-outage-24-billion-or-20-million/ (accessed April 2, 2014).

aside for insurance did not provide financial compensation when it was expected to by the insured company. Instead, Sony will have to pay approximately $171 million in recovery costs and make further investments in its security.[104] While the amount did not financially bankrupt Sony because it is such a large global company, it reduced quarterly earnings and profits. Sony reported the hacking incident in its first quarter 2011 performance earnings report.[105] Public corporations are required to report these events on these reports to the Securities and Exchange Commission when the corporation finds that the event will or has had an adverse effect on earnings. It highlights that the largest companies are still struggling to comprehend completely and manage insurance policies. Companies, especially SMEs, are trying to find a balance between the initial cost and flexibility of insurance policies. Commercial insurance companies are very proactive on what it will or will not provide coverage. In Sony's case, insurance companies will proactively protect their interests and not necessarily the interest of the insured company.

In another recently publicized case, US retail store Target was the victim of a significant data breach sometime between November 27 and December 18, 2013. The intruders illegally accessed the point of sale software and potentially stole up to 40 million users' credit and debit card information plus 70 million users' personally identifiable information such as addresses, email addresses, and phone numbers. Target's insurers will have to settle stolen personal information and credit card claims from tens of millions of shoppers who purchased from the store during that time frame.[106] It was later

[104] Stevens, Tim. "Sony Estimates $3.2b Loss This Year, $171 Million Cost for PSN Breach." Engadget. May 23, 2011. Accessed January 31, 2015. http://www.engadget.com/2011/05/23/sony-estimates-3-2b-loss-this-year-171-million-cost-for-psn-b/.

[105] "Consolidated Financial Results for the First Quarter Ended June 30, 2011." Sony. July 11, 2011. Accessed February 1, 2015. http://www.sony.net/SonyInfo/IR/financial/fr/11q1_sony.pdf.

[106] Yadron, Danny, Paul Ziobro, and Devlin Barrett. "Target Warned of Vulnerabilities Before Data Breach." The Wall Street Journal.

reported that the retail store chain had over $100 million dollars of cyber insurance coverage through $10 million of self-insurance and various layers of commercial insurance by Axis Capital Holdings Ltd, American International Group, and four other unidentified insurers.[107] It is one of the few cybersecurity cases that highlighted a company possessing a significant amount of insurance for cybersecurity breaches.

The cost of Target's data breach and consequential activities was significant. Target has stated that consumers who were affected by the breach would not be responsible for any fraudulent charges and all customers who shopped at Target would receive one free year of credit monitoring. The cost of the investigation and other incident-related activities, as reported in the 4th quarter earnings for Target, came to $61 million before taxes, $44 million of which will be offset by insurance payments.[108] The company was unable to estimate future expenses related to the data breach. Those costs may include fraudulent payments associated with potential claims by credit card companies and card re-issuance costs; costs associated with litigation, investigative and consulting fees; capital investments for remediation activities.[109] These future costs may have material adverse effect on Target's net earnings for 2014 and in the future. It was a company that had some insurance for transferring its cyber risk, but it showed a lack of a recovery planing even though Target may have appeared to be in compliance with its risk

http://online.wsj.com/news/articles/SB10001424052702304703804579381520736715690 (accessed February 16, 2014).

[107] Greenwald, Judy. "Target has $100M of cyber insurance, $65M of D&O cover: Sources." Business Insurance. https://www.businessinsurance.com/article/20140114/NEWS07/140119934?tags=%7C306%7C338%7C299%7C329%7C75%7C76%7C302%7C303 (accessed January 29, 2014).

[108] "Target Reports Fourth Quarter and Full-Year 2013 Earnings 02/26/14." Target-Financial News Release. http://investors.target.com/phoenix.zhtml?c=65828&p=irol-newsArticle&ID=1903678&highlight= (accessed February 27, 2014).

[109] Ibid.

mitigation. The point is especially obvious when the CEO of Target resigned over the poor response by the company to the data breach.[110]

Companies like Sony and Target have financial resources that can maintain financial solvency but smaller companies may not. Companies that especially have large databases of personal identifiable information and financial information are specially vulnerable. Companies face complex issues that may be familiar with the insurance companies but not well understood by the public. The lack of transparency in a relationship between commercial insurers and insureds show that the insurance companies are likely to benefit from the appearance of offering the necessary coverage. When in reality it will reject claims if it does not fulfill every requirement as listed in the written contract. Companies that are proactive in cyber risk mitigation should be financially rewarded compared to companies that are only compliant with broad compliance standards.

This type of risk can be devastating for smaller companies, but few incidents are pulically reported. One of the rare cases publicized in the Wall Street Journal, in 2012, involved a very small business, a mannequin maker and importer, Lifestyle Forms & Displays Inc. The company has annual revenue of $500,000 to $1,000,000 and 100 employees.[111] The company had $1.2 million stolen from its bank accounts in hours through nine online transactions.[112] A problem was only apparent when the head of the

[110] O'Connor, Clare. "Target CEO Gregg Steinhafel Resigns In Data Breach Fallout." Forbes. May 5, 2014. Accessed February 1, 2015. http://www.forbes.com/sites/clareoconnor/2014/05/05/target-ceo-gregg-steinhafel-resigns-in-wake-of-data-breach-fallout/.

[111] "Lifestyle Forms Display CO." Manta. Accessed February 1, 2015. http://www.manta.com/c/mmsrltm/lifestyle-forms-display-co.

[112] Needleman, Sarah. "Cybercriminals Sniff Out Vulnerable Firms." Wall Street Journal. http://online.wsj.com/news/articles/SB10001424052702303933404577504790964060610?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052702303933404577504790964060610.html (accessed January 6, 2014).

finance department was unable to login to the company's banking website. The bank denied any issues with its website, Keilson's three-person IT team decided that the company was hit by a virus, despite having up to date anti- virus software, and worked on the clean-up. The FBI and the New York Police Department visited the company's headquarters to investigate, but there were no follow-up attempts by either organization. After fifteen days of the owner persistently contacting the various banks and its executives to get assistance, the company was able to recover $1.04m of the stolen money. The company was extremely fortunate in retrieving the majority of money in two weeks, but the WSJ did not report if company did not have insurance to cover such unexpected risks. The company was large enough to have a small IT team but it did not have experience in dealing with malicious attacks and communication with third-party service providers such as banks, or law enforcement in these high pressure situations.

While the amount of actual money stolen out of the account did not cause long-term financial damage, the economic cost was significant if one considers the cumulative time and resources of Keilson and his staff shifted away from normal operations in order to recover the stolen money. There can be endless scenarios like the one just discussed, but the incidents can vary in its damage to the victim company. Depending on the timing of these attacks, if money was stolen before payroll was deducted from the operating accounts; it could have an direct and adverse affect on the cashflow. Smaller companies that do not have a team to respond to such events are unlikely to have people who have a technical background or even knowledge of whom to reach out in the events like these. The resources available on the Internet provides a broad range of guidance for companies but it lacks the clarity necessary for companies attempting to manage a crisis as apparent for the mannequin maker.

## Conclusion

One of the tools to provide guidance to a comprehensive risk management strategy is through cyber insurance. It is a growing field within the insurance industry because existing insurance to cover liability does not explicitly provide coverage for losses related to digital assets and losses caused by cyber-related incidents. Data is the new currency in the information economy. This category of insurance will continue to gain traction because companies of all sizes are increasingly relying on technology to conduct business.

Cyber insurance will continue to attract interest as media publicize attention on public companies that experience cyber-related incidents. As awareness grows, the tools deployed in these instances need to become nuanced because there is no perfect cyber solution for companies. Even the largest companies with the deep pockets and departments dedicated to information security have not properly responded to cyber-related incidents. Companies like Target and Sony have lost millions, and at least one top executive has lost their jobs as a consequence of poor response to major cyber breaches. Smaller companies do not have the luxury that large corporations have with large operating accounts and lines of credit to absorb losses. The consequences are potentially dire for SMEs that do not have resources or individuals to rely on to properly managed unexpected and potentially debilitating incident affecting the daily operations.

Small and medium enterprises face disproportionate challenges in managing its cyber risk. SMEs have much less financial resources and adequate human capital to address risk management because it can be viewed secondary to revenue generating activities. It is increasingly necessary because the government has not provided clarity on what the government will provide in these scenarios and putting the onus on the private sector to develop resources to address cyber risk management. Stakeholders such as consumers and investors will increasingly demand that companies are sufficiently addressing cyber risk through a thoughtful risk management strategy. The resources for SMEs to create a comprehensive risk management strategy to address cyber risks are disparate and not necessarily the easiest to understand.

This paper argues that SMEs that are considering incorporating cyber insurance should consider the captive insurance company as the vehicle to provide broad coverage for its liability in cyberspace. The creation of a captive insurance company for SMEs provides the type of control and inherent financial incentive for companies that have insurance be a necessity for transferring some of the risks of operating in cyberspace. Since the parent company is insuring itself, the company will be incentivized to mitigate as much risk as possible and create an adequate response, and recovery plan that will perform in the event of the unexpected loss.

The creation of a captive insurance company provides a financial incentive for parent companies if they obtain the IRS designation of 831 (b) for its captive company. It changes the taxation that is traditionally on the total amount of premium received by only taxation on the investment income. The insurance premium paid by the company will also be tax deductible. The parent company now has money that can be used for reinsurance to provide additional coverage. The combination of the alternative taxation of investment income compared to premium received can be potentially be substantial to a small company with other benefits that include financial incentive to improve its internal cybersecurity.

The most compelling strength of the captive insurance company is that the actual claims process will be efficient and most likely to be beneficial to the insured company. Unlike commercial insurers that will proactively defend its interest against insured companies such as Sony, captive insurance companies are subsidiaries of the parent company. The parent company can draft language that will enable the insured parent company to access the money in the event of a qualified loss. Commercial insurers have not necessarily shown that it will be as amenable as a captive insurance. In cyberspace, the future is unknown with cyber-related losses as the technology and assets evolve. SMEs that wish to have control over the uncertainty of insurance coverage for cyber-related risk may find it appropriate to its needs.

# Bibliography

"2012 Data Breach Investigations Report." Verizon. http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf (accessed February 19, 2014).

"26 U.S. Code § 831 - Tax on Insurance Companies Other than Life Insurance Companies." Legal Information Institute. Accessed January 21, 2015. http://www.law.cornell.edu/uscode/text/26/8

Anderson, Ross, and Tyler Moore. "Information security: where computer science, economics and psychology meet." *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 367, no. 1898 (2009): 2717-2727.

Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." *Computer networks* 54, no. 15 (2010): 2787-2805.

Baker, Wade, A. Hutton, C. David Hylender, J. Pamula, C. Porter, and M. Spitler. "2011 data breach investigations report." *Verizon RISK Team, Available: www. verizonbusiness. com/resources/reports/rp_databreach-investigations-report-2011_en_xg. pdf* (2011): 1-72.

Bolot, Jean, and Marc Lelarge. "Cyber Insurance as an Incentivefor Internet Security." In *Managing information risk and the economics of security*, pp. 269-290. Springer US, 2009.

Bojanc, Rok, and Borka Jerman-Blažič. "An economic modelling approach to information security risk management." *International Journal of Information Management* 28, no. 5 (2008): 413-422.

Brockett, Patrick L., Linda L. Golden, and Whitley Wolman. "Enterprise Cyber Risk Management." *Risk management for the future–Theory and cases* (2012).

"Captive Insurance Companies." National Association of Insurance Commissioners. http://www.naic.org/cipr_topics/topic_captives.htm (accessed February 18, 2014).

Carneiro, Alberto. "Adopting new technologies." *Handbook of business strategy*7, no.

Cleveland, Bruce . "Cyber Liability Insurance â€" As a Cloud Provider Can You Afford Not To Have It?." Bruce Clevelands Rolling Thunder. http://www.interwest.com/rolling-thunder/on-demand/cyber-liability-insurance-as-a-cloud-provider-can-you-afford-not-to-have-it/ (accessed March 31, 2014).

"Commercial General Liability Insurance." Texas Department of Insurance. http://www.tdi.texas.gov/pubs/pc/pcgenliab.html (accessed March 30, 2014).

"Consolidated Financial Results for the First Quarter Ended June 30, 2011." Sony. July 11, 2011. Accessed February 1, 2015. http://www.sony.net/SonyInfo/IR/financial/fr/11q1_sony.pdf.

"Cybersecurity Insurance Workshop Readout Report." Department of Homeland Security. http://www.dhs.gov/sites/default/files/publications/cybersecurity-insurance-read-out-report.pdf (accessed December 17, 2013).

"Cybersecurity Insurance Workshop Readout Report." Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/cybersecurity-insurance-read-out-report.pdf (accessed April 1, 2014).

Fox, Gary A., and Lynn M. McGuire. "Forming a Captive Insurance Company-Understanding the Business and Tax Implications." *Tax Executive* 64 (2012): 149.

"Fundamentals of P/C Reinsurance." Reinsurance Association of America. http://www.reinsurance.org/Fundamentals/ (accessed March 30, 2014).

Greenwald, Judy. "Target has $100M of cyber insurance, $65M of D&O cover: Sources." Business Insurance. https://www.businessinsurance.com/article/20140114/NEWS07/140119934?tags=%7C306%7C338%7C299%7C329%7C75%7C76%7C302%7C303 (accessed January 29, 2014).

Hall, Shanique. "Recent Developments in the Captive Insurance Industry." NAIC. http://www.naic.org/cipr_newsletter_archive/vol2_captive.htm (accessed March 30, 2014).

Henson, Richard, Daniel Dresner, and David Booth. "IASME: Information Security Management Evolution for SMEs." (2011): 1-11.

"How to Determine Whether to Insure Directors and Officers
BY Inc. staff." Inc.com. http://www.inc.com/guides/2010/12/how-to-determine-whether-to-insure-directors-and-officers.html (accessed March 31, 2014).

Jackson, William D., Mark Jickling, and Baird Webel. "The economic impact of cyber-attacks." Congressional Research Service, Library of Congress, 2004.

Katz, David. "In the Trenches of the Cyber War." CFO. October 27, 2014. Accessed January 8, 2015. http://ww2.cfo.com/data-security/2014/10/trenches-cyber-war/.

Kirilov, Rosen. "Effectiveness of the Information Security in the Banks."*Cybernetics and Information Technologies* 6, no. 2 (2006).

"Lifestyle Forms Display CO." Manta. Accessed February 1, 2015. http://www.manta.com/c/mmsrltm/lifestyle-forms-display-co.

Majuca, Ruperto P., William Yurcik, and Jay P. Kesan. "The evolution of cyberinsurance." *arXiv preprint cs/0601020* (2006).

Mcgrath, Maggie. "Target Data Breach Spilled Info On As Many As 70 Million Customers." Forbes. January 10, 2014. Accessed December 27, 2014. http://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/.

National Cyber Security Alliance, Symantec, JZ Analytics . "2012 NCSA / Symantec National Small Business Study." National Cyber Security Alliance. http://www.staysafeonline.org/download/datasets/4389/2012_ncsa_symantec_small_business_study.pdf (accessed February 28, 2014).

Needleman, Sarah. "Cybercriminals Sniff Out Vulnerable Firms." Wall Street Journal. http://online.wsj.com/news/articles/SB10001424052702303933404577504790964060610?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052702303933404577504790964060610.html (accessed January 6, 2014).

O'Connor, Clare. "Target CEO Gregg Steinhafel Resigns In Data Breach Fallout." Forbes. May 5, 2014. Accessed February 1, 2015. http://www.forbes.com/sites/clareoconnor/2014/05/05/target-ceo-gregg-steinhafel-resigns-in-wake-of-data-breach-fallout/.

Orszag, Peter R. *Homeland security and the private sector*. Brookings Institution, 2003.

Paar, Randy, Elizabeth Sherwin, David Elkind, and Kirk Pasich. "A Policyholder's Primer on Insurance." Dickstein Shapiro. http://www.dicksteinshapiro.com/files/upload/Insurance_Coverage_Primer_A_Policyholder's_Primer_on_Insurance.pdf (accessed March 31, 2014).

Ponemon Institute. "Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age." Fierce Markets. http://assets.fiercemarkets.com/public/newsletter/fiercehealthit/experian-ponemonreport.pdf (accessed December 17, 2013).

Schectman, Mark. "When to Disclose A Data Breach: How About Never?." Wall Street Journal. http://blogs.wsj.com/riskandcompliance/2014/03/27/when-to-disclose-a-data-breach-how-about-never/ (accessed April 2, 2014).

Schwarcz, Daniel, and Steven L. Schwarcz. "Regulating Systemic Risk in Insurance." (2014).

Sembhi, Sarb. "An Introduction to Cyber Liability Insurance Cover." An Introduction to Cyber Liability Insurance Cover. Accessed January 14, 2015.

http://www.computerweekly.com/news/2240202703/An-introduction-to-cyber-liability-insurance-cover.

Shetty, Nikhil, Galina Schwartz, Mark Felegyhazi, and Jean Walrand. "Competitive cyber-insurance and internet security." In *Economics of Information Security and Privacy*, pp. 229-247. Springer US, 2010.

Shrestha, Bibeka . "Details Emerge On Ruling Nixing Sony's Cyber Coverage." Law360. http://www.law360.com/articles/515200/details-emerge-on-ruling-nixing-sony-s-cyber-coverage (accessed April 2, 2014).

"Statistics about Business Size (including Small Business)from the U.S. Census Bureau." US Census Bureau . https://www.census.gov/econ/smallbus.html (accessed April 1, 2014).

Stevens, Tim. "Sony Estimates $3.2b Loss This Year, $171 Million Cost for PSN Breach." Engadget. May 23, 2011. Accessed January 31, 2015. http://www.engadget.com/2011/05/23/sony-estimates-3-2b-loss-this-year-171-million-cost-for-psn-b/.

Stoneburner, Gary, Alice Goguen, and Alexis Feringa. "Risk management guide for information technology systems." *Nist special publication* 800, no. 30 (2002): 800-30.

Takahashi, Dean. "The cost of Sony's PlayStation Network outage: $24 billion or $20 million?." VentureBeat. http://venturebeat.com/2011/04/27/the-cost-of-sonys-playstation-network-outage-24-billion-or-20-million/ (accessed April 2, 2014).

"Target Reports Fourth Quarter and Full-Year 2013 Earnings 02/26/14." Target-Financial News Release. http://investors.target.com/phoenix.zhtml?c=65828&p=irol-newsArticle&ID=1903678&highlight= (accessed February 27, 2014).

Taylor, Greg, and Scott Sobel. "A Closer Look at Captive Insurance." The CPA Journal. June 1, 2008. Accessed January 31, 2015. http://www.nysscpa.org/cpajournal/2008/608/essentials/p48.htm.

"TRIA Is Renewed, Finally..."The National Law Review. January 10, 2015. Accessed January 14, 2015. http://www.natlawreview.com/article/tria-renewed-finallyterrorism-risk-insurance-act.

Weisman, Jonathan. "Congress Passes Measure to Cover Terrorism Risk." The New York Times. January 8, 2015. Accessed January 14, 2015. http://www.nytimes.com/2015/01/09/business/renewal-of-federal-terrorism-insurance-clears-congress.html?_r=1.

Wertz, Glenda. "The Ins and Outs of Errors and Omissions Insurance." Insurance Journal News. http://www.insurancejournal.com/magazines/features/2004/07/19/44745.htm (accessed March 31, 2014).

Yadron, Danny, Paul Ziobro, and Devlin Barrett. "Target Warned of Vulnerabilities Before Data Breach." The Wall Street Journal. http://online.wsj.com/news/articles/SB10001424052702304703804579381520736715690 (accessed February 16, 2014).

Zhao, Xia, and Ling Xue. "A Framework of Using Captive Insurance to Streamline IT Control and Compliance Management." *Journal of Information Privacy & Security* 5, no. 3 (2009).

## Cyber Hygiene in Cyberspace

### Introduction

The best network security system, electronic or otherwise, is only as strong as their weakest link, usually humans. However, the natural tendency of most end users is to go against best practices or even common sense when it comes to security. Large and small companies have to manage external threats, but even the best risk management plans may overlook something as simple as managing the behavior of the end-users. In early 2011, the Department of Homeland Security tested to see how many people would plug in a memory stick or install a computer disc randomly found outside on the ground by nearby government buildings. They found that 60% of the memory sticks and CDs were inserted into work computers, and this number increased to 90% when the memory stick or CD case had a government logo.[113] This case out of many reinforces fears about negligent insider threats but offers little on how to change or properly manage the behavior of end-users of computer networks.

This paper will focus on a relatively new concept called “cyber hygiene,” which aims to explore the ways one might mitigate infiltration of computer networks by way of taking advantage of end-users’ propensities. The concept of cyber hygiene could enhance cybersecurity by incorporation of managing end-user behavior rather than over-reliance on automated technology. Small and seemingly insignificant prudent activities by individual end-users could increase the difficulty and amount of time that attackers spend on infiltration. The additional difficulty of infiltrating a system will mitigate the threat posed by criminal hackers. Improving the security through individual end-user will also

[113] Edwards, Cliff, Olga Kharif, and Michael Riley. "Human Errors Fuel Hacking as Test Shows Nothing Stops Idiocy." Bloomberg. June 27, 2011. Accessed June 25, 2012. http://www.bloomberg.com/news/2011-06-27/human-errors-fuel-hacking-as-test-shows-nothing-prevents-idiocy.html.

improve the overall security and the integrity of company networks.

Small medium size enterprises face an outsized penalty for not including cyber hygiene in its risk management strategy. It is a strategic area of security that does not necessarily require substantial investments in technology, it requires focus on designing or re-designing security that takes user propensity into account when mitigating risk such as restricting the number of users with administrator access, and retraining users to become more situationally aware of potential threats from criminal hackers attempting to access the network through stealing their personal information. Cyber hygiene has potential to empower SMEs to take pro-active steps to improving security and confidence of end-users without necessarily investing significant sums of money.

This paper asks the following question: could the application of the concept "cyber hygiene" to a cybersecurity strategy improve the effectiveness of addressing known electronic vulnerabilities of  network's security for SME? The paper consists of four parts. The first part will present a survey of the existing research on human behavior in the context of cybersecurity. The second part will examine the current public literature of federal agencies and defense contractors. The third part will propose a definition of cyber hygiene. The fourth part is the conclusions and recommendations for future research.

## Literature Review

When searching for literature on humans in the context of cybersecurity the majority of the available research focused on insider threats, particularly the prediction, monitoring, and detection of malicious insider users. The available research reflects the opinion of the vast majority of the research's focus on the stakeholders or the technology involved in cybersecurity.

Frank Greitzer of the Pacific Northwest National Laboratory regularly publishes on insider threats in cybersecurity. He defines insider threats as malicious acts carried out by trusted insiders that may benefit the individual but cause harm to the organization. Greitzer argues that there should be more innovative training solutions such as specialized education and awareness workshops and gaming to combat insider threats. [114] It would become approachable while users learn the necessary skills to improve awareness. He also researches the prediction of insider threats and concludes that there should be a framework for predicting possible malicious exploits that uses psychosocial indicators to monitor human behavior in addition to existing cyber indicators of potential abuse of network resources. Some indicators may be observed directly, such as excessive attempts to access a privileged database or running unauthorized software, while others would be inferred or derived from observed data such as registry entries, IDS/IPS events, and firewall logs. Greitzer recommends there should be further research in defining possible precursors of observable cyber and psychosocial indicators, but also acknowledges that it would be a challenge. [115] Psychosocial behaviors related to anger management, stress, or behavior related to arguments with co-workers or management are something to be noted by managers.  It is easier to observe the outliers in excessive attempts to access privileged databases, downloading unauthorized software, and unusual printing patterns. But it is not necessarily enough evidence to indicate a malicious behavior without some contextual understanding of psychosocial indicators of the

[114] Greitzer, Frank L., Andrew P. Moore, Dawn M. Cappelli, Dee H. Andrews, Lynn A. Carroll, and Thomas D. Hull. "Combating the insider cyber threat." *Security & Privacy, IEEE* 6, no. 1 (2008): 61-64.

[115] Greitzer, Frank L., P. Paulson, L. Kangas, T. Edgar, M. M. Zabriskie, L. Franklin, and Deborah A. Frincke. "Predictive modelling for insider threat mitigation." *Pacific Northwest National Laboratory, Richland, WA, Tech. Rep. PNNL Technical Report PNNL-60737* (2008).

individual as well.

Another interesting piece of research related to managing human behavior comes from Ryan West, who focuses on the psychology of end-users in how they evaluate and make decisions regarding security. West finds that the best-designed interface does not improve network security if users ignore warnings, choose poor settings, or unintentionally subvert corporate policies.[116] He argues that there would be more end-user compliance if security system designers created strategies that utilize the psychological principles driving behavior. [117] This concept relies heavily on security software developers to have a high understanding of human-computer interaction and/or user experience development when most focus on automated algorithms and databases of existing viruses. It will take time to develop software or redesign existing software that is not likely to happen in the immediate future. It does not necessarily solve the immediate problem of mitigating end-user security for SMEs.

James Lewis of CSIS wrote one research piece that specifically addresses cyber hygiene without utilizing the term. Lewis shows that 80 to 90 percent of successful breaches of corporate networks required only basic hacking techniques. It also took 85 percent over months to discover such breaches with an average length of five months for such breaches. Australia’s Defense Signals Directorate (DSD) and the US National Security Agency independently surveyed the techniques used to penetrate networks successfully. The DSD discovered that four risk reduction measures blocked most attacks. Agencies and companies implanting these measures saw risk fall by 85% and, in some

[116] West, Ryan. "The psychology of security." *Communications of the ACM* 51, no. 4 (2008): 34-40.
[117] Ibid.

cases, to zero.[118] The four measures were “whitelisting”, which limits only authorized software to run on a computer or network; real-time patching of programs such as PDF readers, Microsoft Office, and web browsers; real-time patching of operating system vulnerabilities such as Microsoft’s Windows, Linux, and Apple’s OS; and minimizing the number of people on a network with administrator privileges.[119] It clearly identifies that the entry point for penetration is through simple methods, and the success rate merely depends on the hackers’ patience and ability to apply such attacks.

To better manage end-user behavior, a number of researchers have proposed methods for measuring and reducing the vulnerability of networked control systems, especially industrial systems such as SCADA (*Supervisory Control And Data Acquisition*), as the starting point for raising the vulnerability threshold. One method recommends surveying key employees involved in the operation and security of control networks and equipment, which would provide a foundation of understanding of which employees are familiar with compliance and security policies. It is something that can be done internally without the additional investment with outside consultants or auditors.

Another widely mentioned alternative is building network systems that remain resilient after an intrusion or an outright attack. Researchers have looked at resiliency as a means of creating and strengthening information systems and organizations to withstand physical and electronic threats caused by hackers. Information technology resilience focuses on stability and quality of service in the face of constant threats to the networking infrastructure. “A resilient control system is one that maintains state awareness and an accepted level of operational normalcy in response to disturbances, including threats of

[118] Lewis, James. "Raising the Bar for Cybersecurity." Center for Strategic and International Studies. csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf (accessed June 17, 2013).
[119] Ibid.

an unexpected and malicious nature." [120] Such resiliency is achieved by fostering individual, community, and system robustness, as well as enhancing adaptability and the capacity for rapid response and recovery.

One of the more specific recommendations for deterring malicious actors is to modify the feedback control loop, which provides monitoring and control capabilities. Data fusion is a method to concentrate or combine data to yield information, and the data loop is realized when humans fuse data together. As such, if there are specific responses from data fusion, an attacker could reverse-engineer the process to understand the system. Therefore, it is beneficial to increase the amount of confusion in a control system to reduce an attacker's ability to manipulate it. [121]

Vince Cerf, known as one of the fathers of the Internet, published a brief commentary on the philosophical aspect of cybersecurity. He acknowledges that the technical solution is impossible to rely on entirely to resolve cybersecurity and reliance on detection and punishment present ethical issues. [122] Instead, he presents a three-prong approach to deal with cyberattacks and other harmful activity in cyberspace: 1) use technology to inhibit harm; 2) seek to detect and identify harmful actors and take mitigating, including legal, action; 3) use moral-suasion when all else fails.[123] He specifically recommends that within moral-suasion, there should be motivators for users that practice good cyber hygiene. Cyber hygiene implemented by policy and training should reduce cyber insurance premiums because the insured had taken precautionary measures to mitigate risk. Parties that make that kind of commitments should be

[120] Rieger, C. G., D. I. Gertman, and M. A. McQueen. 2009. "Resilient Control Systems: Next Generation Design Research."IEEE, .

[121] Ibid.

[122] Cerf, Vinton G. "First, do no harm." *Philosophy & Technology* 24, no. 4 (2011): 463-465.

[123] Ibid.

rewarded assuming, they are trustworty or can substantiate their commitments.[124] He broadly points to economic incentives to promote the incorporation of cyber hygiene and did not elaborate further on other possible incentives. The example of using reduced insurance premium is a relavant example because cyber insurance market is growing with companies of all sizes. Examples of good cyber hygiene by Cerf 1) non-reusable passwords such as cryptographically generated passwords.[125] These one-time passwords are generated by hardware tokens. One of the most well-known tokens is the RSA SecurID; these are the ubiquitous fobs found on the key chains belonging to many corporate and government employees. 2) introduction of the Domain Name System Security technology to improve the integrity of mapping domain names to Internet Protocol addresses.[126] While most Internet users are familiar with domain names that end such as '.com, .gov, .org' these domains only lead into the actual IP address to the website. Moreover, the domains do not always correspond to numerical addresses assigned to users by Internet service providers. The lack of transparency between the domain names and IP address enables malicious actors to mask their true identity. 3) open source software with the expectation that many would identify and repair vulnerabilities.[127] Cerf agreed that one was debatable because of the assumption of the good will and devotion to the use of the open source software. Wikipedia is an example of open-source collaborative encyclopedia that has a high participation in identifying and correcting incorrect entries quickly. It is not impossible, but it would require significant user adoption. Moral suasion is best helped by the transparency of open-source

[124] Ibid.

[125] Ibid.

[126] Ibid.

[127] Ibid.

collaboration between actors in cyberspace.

Other researchers make references to the phrase cyber hygiene but do not go into depth in specifically in defining or analyzing cyber hygiene. Some researchers referenced instituting cyber hygiene education initiatives.[128] One of the minority research pieces stated that over 80% of attacks can be dealt with through basic cyber hygiene, such as patches, passwords, anti-malware, and firewalls.[129] Even when these tools are put in place if regular maintenance avoided then those tools becomes useless. The authors do not substantiate the percentage in the book. It does voice support for promoting a culture of cyber hygiene and vigilance, with people and organizations following security policies, using strong passwords, regularly applying security patches would make attackers' work more difficult.[130] Further research needs to be conducted on the implementation of cyber hygiene in the face of ever-changing cybersecurity threats.

**Examining Existing Cyber Hygiene Literature**

One of the useful steps in raising the bar for cybersecurity vulnerabilities is to examine the current strategies and opinions of federal organizations and government contractors towards human behavior in cybersecurity. Doing so will create a baseline of how organizations with the most responsibility for defending against basic exploitations. The following section will examine publically available documents such as white papers, capabilities literature, and published interviews with a select number of large government contractors, small 8(a) designated government contracting firms, and major US

[128] Sood, Aditya K., and Richard J. Enbody. "Crimeware-as-a-service—A survey of commoditized crimeware in the underground market." *International Journal of Critical Infrastructure Protection* (2013).
[129] MacKinnon, Lachlan, Liz Bacon, Diane Gan, Georgios Loukas, David Chadwick, and Dimitrios Frangiskatos. "Cyber Security Countermeasures to Combat Cyber Terrorism."
[130] Ibid.

government organizations managing critical infrastructure. [131]

The government contractors and federal organizations selected were: contractors Lockheed Martin, Northrop Grumman, General Dynamics, Booz Allen Hamilton, and SAIC; ASCRC Research and Technology Solutions LLC, Four LLC, Bowhead Science and Technology LLC, Cherokee Nation Technology Solutions LLC, and TKC Global Solutions; and the Department of Defense, Department of Homeland Security, and Department of Transportation.

The government contractors were selected because these companies hold significant cybersecurity/information technology contracts with the federal government. Since 85% of the country's critical infrastructure is owned and operated by the private sector, it is important to examine the private sector's approach towards cybersecurity.[132] Government contractors are held to much more rigorous standards, with laws such as the Federal Acquisition Regulations, as opposed to regular contractual agreements typically implemented by companies in the private sector. The smaller 8a contracting firms were selected from Washington Technology's 2014 largest 8a contractors list based on revenue in 2013 from IT contracts awarded by the federal government. The top five firms listed were chosen for evaluation.

The federal organizations chosen for their relative importance in critical infrastructure and dependence on cybersecurity to protect their information and systems. The management of the energy, defense, finance, transportation, and telecommunications

[131] 8(a) is a designation for government contracting firms that are owned and managed by socially and economically disadvantaged individuals. There are a variety of requirements including the owner's assets must be under $4 million dollars, the adjusted gross income of the owner must less than $200,000 at the time of the application, and the company must have a North American Industry Classification code that meets the definition of small business by the Small Business Administration.

[132] Government Accountability Office. TECHNOLOGY ASSESSMENT Cybersecurity for Critical Infrastructure Protection. www.gao.gov/new.items/d04321.pdf (accessed July 15, 2012).

sectors are vital to the country's national security and well-being.

**Findings**

A comparison of official views of the public and private sectors will establish a public dialog on human behavior in the cybersecurity equation and reveal whether the term "cyber hygiene" is being utilized in the world by organizations. In cases where organizations use the term "cyber hygiene", a definition is established based on its usage in publicly available documents, which will show areas of consensus or gaps in cybersecurity positions and tactics in terms of the most basic vulnerabilities of these critical networks.

Many federal departments have at least one document explicitly stating its views on security and overall strategy. There is also a variety of materials that include testimonies that further clarify or update memos on their cybersecurity strategies.

Public documentation of these government contracting companies' cybersecurity strategies was pieced together from public comments and documentation other than formal strategies. Company websites were reviewed for any public documentation of their strategies or tactics, as were public interviews with company executives and sponsored researchers.

*Lockheed Martin*- A search on Lockheed Martin's website did not show a dedicated document for cyber hygiene. The site lists a variety of services that it offers, including security awareness, training, and education; red and blue team testing; and security compliance reviews. On the front page of the company's product listing are training tools that mimic human behavior and fragilities to prepare users to be able to counter live threats. It does not mention list training tools for end-users.[133] In addition, four white papers are published on the Information Technology Group’s website.[134] One specifically focuses on cloud computing security, though most of its recommendations in regards to human behavior were relatively benign. Lockheed Martin states that any government organization’s security policies should extend to users accessing applications. It also mentions that systems, staff, training, and policies should be assessed and adjusted over time.[135]

Another white paper focuses on computer-network defense, specifically on advance persistent threats.[136] Traditionally, most organizations have relied on technologies and processes implemented to mitigate risks associated with automated viruses and worms, and not necessarily manually-operated APT intrusions. Responding after as intrusion is based on two flawed assumptions: responses should happen after a security breach, and that the breach was based on a fixable flaw.  One study mentioned in the white paper found that end- users of computer networks are directly targeted for their access to sensitive information. The paper presents a specific solution called the intelligence-driven computer network defense, which is a risk management strategy that includes analysis of adversaries and their capabilities, objectives, doctrine, and limitations. It then presents a new model for such intrusions, which focuses on a higher

[133] "Cyber Solutions." Lockheed Martin. http://www.lockheedmartin.com/us/products/cyber-solutions.html (accessed June 18, 2013).

[134] "Cyber Security." Lockheed Martin. http://www.lockheedmartin.com/us/what-we-do/information-technology/cyber-security.html (accessed June 18, 2013).

[135] Lockheed Martin. Getting Secured in the Cloud. www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/Getting-Secure-in-the-Cloud.pdf (accessed July 15, 2012).

[136] Hutchins, Eric, Michael Cloppert, and Rohan Amin. "Intelligence-Driven Computer Network Defense." Lockheed Martin. www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf (accessed June 17, 2013).

level of strategy for computer network defensive measures. It does not mention anything regarding raising the level of end user vulnerabilities.

Rick Doten, Chief Scientist at Lockheed Martin's Center for Cyber Security Innovation, was asked in an interview about non-technical aspects of cybersecurity. Doten said, “Technology is always the easy part, which, unfortunately, is why it’s always the first solution that’s thrown at a problem.” He focused on the necessity to find the right people and create the right processes for proper leadership. Once proper direction is established, then a move from a technology-driven approach towards risk-based approach can take place. [137]

*Northrop Grumman (NG)*- The company’s cybersecurity website lists a variety of literature promoting the strength of its employees, software, and services.[138] A published interview with NG’s Chief Information Security Officer (CISO) includes a line mentioning the company’s belief in a top-down approach driven by its top executive. NG acknowledges the end-user as a weakness in the network or, as the CISO described in the interview, “the IT supply chain”. It also talked about the attack tactics such as spear phishing, a digital form of social engineering that uses authentic looking but fake requests information from users, used to target individuals in organizations.[139] Spear phishing was the number one vector for exploiting weaknesses in governments and business. The company itself reviews its security plan, training and awareness, and countermeasures

[137] "The Stand: Cybersecurity -- Government Computer News." Government Computer News: Latest tech product reviews, mobile technology updates and security news for federal IT, state IT and local government IT -- Government Computer News. http://gcn.com/pages/custom/stand-cybersecurity.aspx (accessed August 12, 2012).

[138] "Cybersecurity Literature." Northrop Grumman Corporation - The Value of Performance. http://www.northropgrumman.com/cybersecurity/literature/ (accessed August 12, 2012).

[139] Wilshusen, Gregory C.. "CYBERSECURITY- Threats Impacting the Nation." Government Accountability Office. www.gao.gov/assets/600/590367.pdf (accessed June 17, 2013).

against spear phishing.  The Most notable details was that the company spear phishes its employees to test their awareness.[140]

*General Dynamics (GD)*- There was no literature found on the company's website. The website provided a very basic overview of services and products, but none of the information reference managing neither human behavior nor cyber hygiene. In an interview with Bill Ross, Director of Cyber Mission Assurance Systems, he said that the culture was the toughest problem to tackle because there needs to be a balance between access to information, transparency, and end user responsibility. Ross said, "You are only as good as your weakest link, so teaching people the culture of what it means to be stewards within the cyber domain is going to be a huge challenge." [141]

*Booz Allen Hamilton (BAH)*- The company had a substantial amount of published thought pieces on cybersecurity that included reports, surveys, articles, and videos. There were no results from a search on the company's website for literature that focused on the human behavior aspect of cybersecurity. [142] The cyber solutions capabilities brochure claims to provides training to clients through the Booz Allen Cyber Training Center. Training included defensive and offensive techniques, so clients can learn to think like the enemy and defend themselves at the same time.[143] BAH contributed to a report released by the Information Assurance Technology Analysis Center, listed under the

[140] Federal Computer Week. "The Stand." Northrop Grumman on Cybersecurity. http://www.northropgrumman.com/cybersecurity/presentations/assets/STAND_Cyber_NG.pdf (accessed August 12, 2012).

[141] "The Stand: Cybersecurity -- Government Computer News." Government Computer News: Latest tech product reviews, mobile technology updates and security news for federal IT, state IT and local government IT -- Government Computer News. http://gcn.com/pages/custom/stand-cybersecurity.aspx (accessed August 12, 2012).

[142] "Cyber Solutions." Booz Allen Hamilton. http://www.boozallen.com/consulting/prepare-for-whats-next/cyber (accessed August 17, 2012).

[143] "Harness the Power." Booz Allen Cyber Solutions Network. www.boozallen.com/media/file/CSN_Brochure.pdf (accessed August 15, 2012).

Department of Defense findings.

*Science Applications International Corporation (SAIC)* - While most of SAIC's website was similar to the previously mentioned government contractors, with its proprietary cybersecurity products and services. One of the search results within the company website was an article that talked about five things that kept the executives up at night, and one of the five items was the lack of proper workforce training. The executive argued that the best return on investment in cybersecurity is by training the workforce because it has the greatest range of threats from bad user practices to social engineering. The article listed its proprietary iSecure training application that it requires its employees to use every year. [144]

*ASCRC Research and Technology Solutions LLC*- The company lists its broad areas of expertise such as information technology, decision support, and programmatic support. It also has a list of federal agency clients and contracted services. It does not reference specific cybersecurity but in a search for job openings, the firm has a position for a cyber security compliance officer. The officer is responsible for managing all aspects of compliance internally and with external clients.[145] There are references to developing and implementation of measures to meet compliance and monitoring so there is a possibility of developing measures that could incorporate cyber hygiene. Within the job posting, it referenced an internal group called the Security Working Group that is to provide input on security goals and integrate security goals with business goals.[146]

*Four Inc*- It is a woman-owned company that provides technology solutions. It

[144] Giesler, Bob . "Five Issues in Cyber That Cause Sleepless Nights." SAIC. www.saic.com/news/pdf/saic-science-to-solutions-2009.pdf (accessed August 5, 2012).

[145] "Job Openings." ASRC Federal. Accessed March 31, 2015.

[146] Ibid.

does not list any specific capabilities within cybersecurity. It does show that the company offers security products from cyber security vendors such as Mcafee, VMware, Lumeta, Forescout.[147]

*Bowhead Science and Technology LLC*- The company listed information assurance, program protection, and anti-tamper as critical capabilities within cyber security. It does not go into greater detail about its thought leadership of cybersecurity. Job descriptions also posted  did not reveal any significant internal organization inclusive of security or compliance. It showed that it will hire contract employees to provide cyber security services in order to fulfill certain government contracts awarded to the company such as network security engineer identifying software and solutions for developing Intrusion Detection Architecture for NSWC Crane networks. [148]

*Cherokee Nation Technology Solutions LLC*- It lists a multitude of technology services including management information systems, network infrastructure management, and software development but excludes cyber security as an offering.[149] There is a lack of insight into the company's security. The available job postings also do not indicate any current job vacancies internally focused on cybersecurity.

*TKC Global Solutions LLC*- This company lists a broad set of capabilities within its cybersecurity holdings. It includes services under these categories: monitoring, detection, analysis and response, and recovery. It mentions the ability to provide services for cloud based platform, bring your own devices (BYOD) , and managing insider threats. It lists specific cybersecurity services provided to Bureau of Indian Affairs,

[147] "Four Inc." Products. Accessed April 1, 2015.
[148] "Bowhead Holding Company Network Security Engineer Job in Crane, IN." Glassdoor. Accessed April 1, 2015.
[149] "Cherokee Nation Technology Solutions." Cherokee Nation Technology Solutions. Web. 2 Apr. 2015.

Department of Homeland Security, and Defense Information Systems Agency, and US Army.[150] It shows a very clear set of capabilities within cybersecurity and publicly lists the manner in which the company has supported government agencies in their cybersecurity efforts. It may be the smallest 8a contractor of the group, but it presents the information as clearly as ASCRC, a larger competitor in the 8a market for technology contracts with the government.

*Department of Defense*- The DOD's Strategy for Operation in Cyberspace stated the necessity to address human behavior related vulnerabilities and potential threats with "cyber hygiene." The analogy defined an activity that was to be regularly practiced by users and administrators to maintain information security. It stressed that maintenance for users and administrators, secure network design and implementation, and proper management of the network, were all important factors. The combination of those parts creates a holistic approach towards a secure network.[151]

Most importantly, it listed people as the DOD's first line of defense to reducing intentional and unintentional insider threats. The tactics listed to strengthen its first line of defense included communication, personnel training, new technologies, and processes. The cumulative effect of integrating these categories will improve end user security, through educated end-users with clearer understanding of procedures to ensure that they will not be exploited by sophisticated hackers. It also mentioned the desire for the DOD to foster a culture of information assurance.[152] The creation of this culture to increase individual responsibility and deter malicious insiders by affecting behaviors and norms

[150] "Our Customers." TKC Global. Web. 2 Apr. 2015. .

[151] Department of Defense. Department of Defense Strategy for Operating in Cyberspace ."www.defense.gov/news/d20110714cyber.pdf (accessed July 15, 2012).

[152] Ibid.

with imposed higher costs to operate.

The National Cyber Range was listed as one of the tools to execute realistically, quantifiable assessments of the country's cyber research. The Cyber Range is a national research for individuals to test technologies and systems in a contained environment. Researchers will look for vulnerabilities from component to the system level, and from events such as buggy code, misconfigurations, and user actions in realistic situations. [153]

The Information Assurance Technology Analysis Center (IATAC) under the direction of the DOD created a report, with the guidance from BAH, on the state of the environment of measuring cybersecurity and information assurance in 2009. One section of the report was dedicated to measuring security knowledge and implementation of the security knowledge. In a Master thesis, Measuring Information Security Awareness by Johnny Mathisen, he argued that there is a discrepancy between what people say and what they do when it involves measuring the change in human behavior, especially when it comes to information security education and training. The reported Mathisen's metrics as well as custom metrics developed by other organizations, some of the examples listed were the Internet Security Forum, United Kingdom (UK) Chapter of the Information Systems Security Association, US Army, and the Gartner Group. Mathisen's nine metrics- % of employees completed the necessary security training, # of reported security incidents, % of clean desks at COB, % of waste paper that shredded, $ of illicit traffic on the internal network, % of weak user passwords, # of hits on web pages about security, # of requests for information assistance by the security office, and customer satisfaction. [154]

[153] DARPA. "The National Cyber Range: A National Testbed for Critical Security Research." White House. http://www.whitehouse.gov/files/documents/cyber/DARPA%20-%20NationalCyberRange_FactSheet.pdf (accessed August 14, 2012).

[154] Bartol, Nadya, Brian Bates, Karen Mercedes Goertzel, and Theodore Winograd. "Measuring Cyber

Some of the challenges to establishing a program to measure information security properly revealed in a 2007 Forrester survey of 19 Chief Information Security Officers about their current IT security practices. The top challenges for implementation were the following: Finding the right metrics and translating the security metrics into "business language." Forrester's analysts also noted the following observations- metrics were focused on operational and project status, and driven by compliance concerns, confusion about security measurements with metrics, and security metrics collected were not useful for their intended purpose or audience.[155]

*Department of Homeland Security (DHS)*- DHS published Cybersecurity Strategy for the Homeland Security Enterprise in November 2011. The strategy provided an outline to protect critical systems and assets essential to the United States. One of the sections of the strategy was dedicated to the promotion of cybersecurity knowledge. Some of the objectives included education and awareness campaigns that were created to help increase awareness among the workforce. Some of the campaigns are DHS has the "Stop. Think. Connect" campaign, Cyber Awareness Coalition; Stay Safe Online; National Cyber Security Awareness Month activities across all levels around the country. There should also be best practices and guidelines for actions individuals to strengthen individual defenses. Moreover, mechanisms that notify users that devices and systems have weakness or are infected, enabling them to take action. [156]

While the majority of the recommendations revolved around the technology, there was a section devoted to the usage of the technology. Some of the items listed to reduce

Security and Information Assurance." Information Assurance Technology Analysis Center. iac.dtic.mil/iatac/download/cybersecurity.pdf (accessed August 15, 2012).

[155] Ibid.

[156] "Blue Print for a Secure Cyber Future." Department of Homeland Security. www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf (accessed August 13, 2012).

(end user) vulnerabilities were a security product evaluation or validation regimes and to improve usability. Designing trusted technology that is easy to use, administer, customizable, and to perform as expected. Some of the core capabilities are requirements and guidelines that indicate acceptable characteristic for assembly, configuration, operations administration, and performance such as the human computer interface standards by American National Standards Institute and UsabilityNet. Finally, to improve usability, create studies to determine the aspects of security technology that lead to rapid adoption and standardization within relevant user communities. [157]

*Department of Transportation (DOT)*- There was no official strategy listed on the website for the Office of the Chief Information Officer, DOT. There was no information on the DOT's website alluding to human behavior in the cybersecurity. The website listed some general cybersecurity priorities for the DOT: to follow federal cybersecurity initiatives such as the National Security Presidential Directive 54/ Homeland Security Presidential Directive 23; to enhance the support for the DOT Cyber Security Management Center, enhance cyber incident response and situational awareness of the DOT cyber infrastructure, and improve information sharing capabilities with the DHS. The office of CIO will need to enhance verification and validation functions as required by statute, expand the use of OMB reporting tools. And increase the use of automation tools in order to reduce verification and validation burden on DOT system and service owners. The Office will need to modernize the DOT's certification and accreditation program by using new technology and processes, expand the use of Cyber Security Assessment and Management tool, and enhance data quality reviews to identify and correct performance gaps. Finally, the Office will need to enhance compliance with

[157] Ibid.

federal statutes and requirements to protect privacy information and ensure closure of privacy performance gaps. [158]

*Analysis*

These organizations show varying degrees of sophistication of presentation of its thought leadership in its external and internal management of cybersecurity and human behavior. The much larger contractors and government organizations included significant thought leadership on cyber hygiene, its application, and definitions. It shows the largest public and private organizations are aware of the concept and more likely to take the concept into consideration with its implementation. It should not be surprising these organizations have published documentation because of their substantial resources.

The 8a contractors selected to represent small medium enterprises showed a varying degree of sophistication in cybersecurity much less cyber hygiene. ASRC and TKC were the companies with the most sophisticated presentation of cybersecurity offerings and references to services that can be related to cyber hygiene. The lack of sophistication in cybersecurity provides an area for further research and publicity for improving the broad spectrum of SMEs' working knowledge and application of cybersecurity practices, especially cyber hygiene. Cyber hygiene should be broken down for SMEs for technical, organizational, and individual application through education and training.

## Proposed Definition for Cyber Hygiene

Cybersecurity defense tactics will have to continue to be fluid while strategies are solidified. The defense is no longer a line drawn in the sand; it is drawn in space, and it

[158] "Cybersecurity | Office of Chief Information Officer." Home | U.S. Department of Transportation. http://www.dot.gov/cio/cyber.html (accessed August 5, 2012).

must regularly be redrawn to prevent unauthorized access to networks. Many public and private sector leaders have talked about cyber hygiene and presented examples of cyber hygiene, but none have stated a clear definition for it. The paper proposes the following definition as a starting point in clarifying term 'cyber hygiene.' Cyber hygiene has very specific characteristics mentioned in various published documents but not explicitly codified.

*Authorized software and devices*- the Individual user only using pre-approved software and devices to transmit information within and outside of the network.[159]

*Individual user security maintenance*- Individuals user is regularly updating security codes, questions (passwords, pins, personal identification information), and virus patches for applications, systems, and networks.[160]

*Actively reject exploitations*- Individual user actively rejecting all types of attempts by hackers or any other unauthorized individuals from gaining accessing and exploiting the user's access privileges. It requires education and training on how to recognize such attempts.

*Planned response*- If an individual user notices unfamiliar activity in their daily activity within the network, the user should know whom to contact to report the incident immediately and how to document the unauthorized activity.

These four types of characteristics succinctly define what cyber hygiene in an analogous definition or at least building blocks to a formal definition understood by business managers of small and medium businesses. The definition extends the

[159] "CSIS: 20 Critical Security Controls: Version 4.0." SANS Information, Network, Computer Security Training, Research, Resources. http://www.sans.org/critical-security-controls/guidelines.php (accessed June 19, 2013).

[160] Brennan, John. "Cybersecurity Awareness Month Part III | The White House." The White House. http://www.whitehouse.gov/blog/Cybersecurity-Awareness-Month-Part-III (accessed June 19, 2013).

responsibility of maintaining network security from abstract organizational policy to individual user responsibility. It also lists specific areas previously mentioned in the paper as actual exploitations. The increased security awareness of the importance of ongoing maintenance will raise the bar for hackers who attempt to access privileged networks. These activities are not beyond the capabilities of individual users at all levels of an organization.

Researchers will have to discover which metrics is appropriate for organizations to create appropriate baselines for user and system responsibilities for reducing network vulnerabilities.

## Conclusion

As much interest in cybersecurity research increases, there should also be a consideration in demystifying cybersecurity concepts and uncovering the best practices for successful technical and non-technical cybersecurity tactics. The proposed definition of the cyber hygiene would be important for policy makers and business leaders to have a better understanding of the term while reducing the casual use of the term in the media. The proper understanding cyber hygiene could lead to better policy to address the cybersecurity tactics.

While there is substantive research on cybersecurity, there is still a significant amount of room for a variety quantitative and qualitative research in managing end-user activity in cyberspace and reducing vulnerabilities around them. Developing better cyber security responses will rely on further research in the end user's psychology, user interface, system design, cybersecurity policies and organization culture.[161] These are

[161] Enrici, I., M. Ancilli, and A. Lioy. 2010. "A Psychological Approach to Information Technology Security."IEEE, .

some of the issues that will need to be investigated further to improve the understanding of the concept and its application for companies.

The evidence from research points to some anecdotal awareness of the vulnerability of individual user behavior in cybersecurity across the public and private sectors, with variance between the large and smaller government contracting companies. The simpler cost-saving tactic of applying the cyber hygiene concept goes against the reason government contracting firms providing only technical cybersecurity solutions. Government contracting firms should consider promoting this concept because it increases the value of other tools and services required by the government organizations. While it is not in the interest of contractors to provide such services, it is part of their fiduciary duty to improve the overall security of government networks.

Cyber hygiene is a simpler, more cost-effective tactic for organizations of all size to incorporate in its network security policy. It can certainly increase the value of cybersecurity without necessarily significantly raising the cost of cybersecurity investment. It will enhance security by reducing the expected areas of opportunity for hackers. It can reduce the risk of hackers attempting to social engineer their way into breaking into the network as well as reduce the risk of insider threats such as disgruntled employees. These two types of threats are necessary to manage, but technical solutions do not mitigate as much as it could when combined with cyber hygiene.

All organizations should consider expanding on its cybersecurity strategy to include cyber hygiene as a cost-effective way to increase the end-user vulnerabilities in very sensitive systems and networks. As larger companies and government contractors embrace cyber hygiene, it will set an example for other small and medium size businesses. It is especially important for small and medium sized businesses to embrace the concept since most companies in the US are comprised of small and medium size businesses. By making a standardized definition is a start for small and medium size businesses to understand advance topics underneath the broader term of cybersecurity.

# Bibliography

Atkinson, R. D. 2010. "The Internet Economy 25 Years After. Com: Transforming Life and Commerce." Information Technology and Innovation Foundation.

Bartol, Nadya, Brian Bates, Karen Mercedes Goertzel, and Theodore Winograd. "Measuring Cyber Security and Information Assurance." Information Assurance Technology Analysis Center. iac.dtic.mil/iatac/download/cybersecurity.pdf (accessed August 15, 2012).

"Bowhead Holding Company Network Security Engineer Job in Crane, IN." *Glassdoor*. Web. 1 Apr. 2015.

Boyce, Michael W., Katherine Muse Duma, Lawrence J. Hettinger, Thomas B. Malone, Darren P. Wilson, and Janae Lockett-Reynolds. 2011. "Human Performance in Cybersecurity." Proceedings of the Human Factors and Ergonomics Society Annual Meeting 55 (1): 1115-1119.

"Capabilities for Cybersecurity Resilience." MITRE. https://register.mitre.org/sr/files/fonash.pdf (accessed August 5, 2012).

Censky, Annalyn. "Internet Accounts for 4.7% of U.S. Economy." CNNMoney. March 19, 2012. Accessed June 25, 2012.
http://money.cnn.com/2012/03/19/news/economy/internet_economy/index.htm.
Center for Strategic and International Studies. Significant Cyber Incidents Since 2006. Accessed June 25, 2012.
http://csis.org/files/publication/120504_Significant_Cyber_Incidents_Since_2006.pdf.
"Cherokee Nation Technology Solutions." *Cherokee Nation Technology Solutions*. Web. 2 Apr. 2015.

Clarke, R. A. and R. K. Knake. 2010. Cyber War: The Next Threat to National Security and what to do about it HarperCollins.

Creery, A. and EJ Byres. 2005. "Industrial Cybersecurity for Power System and SCADA Networks."IEEE, .

"Cybersecurity at Risk." New York Times . http://www.nytimes.com/2012/08/01/opinion/cybersecurity-at-risk.html (accessed August 17, 2012).

"Cybersecurity Literature." Northrop Grumman Corporation - The Value of Performance. http://www.northropgrumman.com/cybersecurity/literature/ (accessed August 12, 2012).

"Cyber Solutions." Booz Allen Hamilton. http://www.boozallen.com/consulting/prepare-for-whats-next/cyber (accessed August 17, 2012).

DARPA. "The National Cyber Range: A National Testbed for Critical Security Research." White House. http://www.whitehouse.gov/files/documents/cyber/DARPA%20-%20NationalCyberRange_FactSheet.pdf (accessed August 14, 2012).

Department of Defense. Department of Defense Strategy for Operating in Cyberspace . www.defense.gov/news/d20110714cyber.pdf (accessed July 15, 2012).

Department of Homeland Security. Fiscal Year 2012 Budget Request. Accessed June 25, 2012. http://www.dhs.gov/xlibrary/assets/budget-bib-fy2012-overview.pdf.

Department of Homeland Security. Written Testimony of DHS Secretary Janet Napolitano for a Senate Committee on Homeland Security and Governmental Affiars Hearing on The President's Fiscal Year 2013 Budget Request for The Department of Homeland Security. March 21, 2012. Accessed June 25, 2012. http://www.dhs.gov/ynews/testimony/20120321-s1-fy13-budget-request-hsgac.shtm.

Edwards, Cliff, Olga Kharif, and Michael Riley. "Human Errors Fuel Hacking as Test Shows Nothing Stops Idiocy." Bloomberg. June 27, 2011. Accessed June 25, 2012. http://www.bloomberg.com/news/2011-06-27/human-errors-fuel-hacking-as-test-shows-nothing-prevents-idiocy.html.

Enrici, I., M. Ancilli, and A. Lioy. 2010. "A Psychological Approach to Information Technology Security."IEEE, .

Etzioni, A. 2011. "Cybersecurity in the Private Sector." Issues in Science and Technology 28 (1): 58.

Giesler, Bob . "Five Issues in Cyber That Cause Sleepless Nights." SAIC. www.saic.com/news/pdf/saic-science-to-solutions-2009.pdf (accessed August 5, 2012).

Government Accountability Office. "INFORMATION SECURITY -Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses." .. www.gao.gov/new.items/d07837.pdf (accessed August 13, 2012).

Government Accountability Office. TECHNOLOGY ASSESSMENT Cybersecurity for Critical Infrastructure Protection. www.gao.gov/new.items/d04321.pdf (accessed July 15, 2012).
Haack, Jereme A., Glenn Fink, Wendy Maiden, David McKinnon, and Errin Fulp. "Mixed-Initiative Cyber Security: Putting Humans in the Right Loop." Accessed June 25, 2012. http://u.cs.biu.ac.il/~sarned/MIMS_2009/papers/mims2009_Haack.pdf.

"Harness the Power." Booz Allen Cyber Solutions Network. www.boozallen.com/media/file/CSN_Brochure.pdf (accessed August 15, 2012).

Institute of Homeland Security Solutions. Cyber Security: Exploring the Human Element.

March 8, 2011. Accessed June 25, 2012.
http://sites.duke.edu/ihss/files/2011/12/CyberForumSummary1.pdf.

Institute of Homeland Security Solutions. Cyber Security: Exploring the Human Element. March 8, 2011. Accessed June 25, 2012.
http://sites.duke.edu/ihss/files/2011/12/CyberForumSummary1.pdf.

Jackson, William. The Security Singularity: When Humans Are the Biggest Threat to Information Systems -- Government Computer News. September 23, 2011. Accessed June 25, 2012. http://gcn.com/articles/2011/09/23/cybereye-security-singularity-human-threat.aspx.

"Job Openings." *ASRC Federal*. Web. 31 Mar. 2015.

Kriz, D. 2011. "Cybersecurity Principles for Industry and Government: A Useful Framework for Efforts Globally to Improve Cybersecurity."IEEE, .

Lewis, J. A. 2008. "Securing Cyberspace for the 44th Presidency." Center for Strategic and International Studies 8.

Lockheed Martin. Getting Secured in the Cloud.
www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/Getting-Secure-in-the-Cloud.pdf (accessed July 15, 2012).

Napolitano, Janet. "Testimony of DHS Secretary Janet Napolitano before the Senate Committee on Homeland Security and Governmental Affairs for a hearing entitled “Securing America's Future: The Cybersecurity Act of 2012”." Department of Homeland Security. www.dhs.gov/news/2012/02/16/testimony-dhs-secretary-janet-napolitano-senate-committee-homeland-security-and (accessed August 5, 2012).

One NSF INVESTMENTS. SECURE AND TRUSTWORTHY CYBERSPACE (SaTC). Accessed June 25, 2012. http://www.nsf.gov/about/budget/fy2013/pdf/43_fy2013.pdf.
"Our Customers." *TKC Global*. Web. 2 Apr. 2015.

Pfleeger, S. L. and D. D. Caputo. 2012. "Leveraging Behavioral Science to Mitigate Cyber Security Risk." .

Ponemon Institute LLC. 2011 Cost of Data Breach Study-United States. March 2012. Accessed June 25, 2012. http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Mar_worldwide__CODB_US.

Rieger, C. G., D. I. Gertman, and M. A. McQueen. 2009. "Resilient Control Systems: Next Generation Design Research."IEEE, .

Schwartz, Mathew J. "InformationWeek: The Business Value of Technology." Informationweek. May 31, 2011. Accessed June 25, 2012. http://www.informationweek.com/news/government/security/229700151.

Stern, Matt. "And Now for Something Completely Different: Influencing Threat Behavior." US CERT. N.p., n.d. Web. 13 Aug. 2012. <http://www.us-cert.gov/GFIRST/presentations/2011/And

"The Stand: Cybersecurity -- Government Computer News." Government Computer News: Latest tech product reviews, mobile technology updates and security news for federal IT, state IT and local government IT -- Government Computer News. http://gcn.com/pages/custom/stand-cybersecurity.aspx (accessed August 12, 2012).

Waterman, Shaun. "Pentagon Expected to Increase Spending on Cybersecurity." The Washingtion Times. February 13, 2012. Accessed June 25, 2012. http://www.washingtontimes.com/news/2012/feb/13/pentagon-expected-increase-spending-cybersecurity/.

White House. Cyberspace Policy Review. Accessed June 25, 2012. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

The White House." Remarks by the President on Securing Our Nation's Cyber Infrastructure" May 29, 2009. Accessed June 25, 2012. http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

"Industrial Cybersecurity for Power System and SCADA Networks."IEEE,

Wolf, C. 2011. "The Role of Government in Commercial Cybersecurity."

## Conclusion

Cyberspace is an evolving environment that provides significant opportunities and risks. SMEs have access to greater innovation, cost reduction, and marketing opportunities than ever before. The lack of governance in cyberspace has provided opportunities taken advantage by SMEs, but few are managing the risks related to the lack of law and order in cyberspace. SMEs need develop tools to manage risk because evident vulnerabilities will be eventually exploited by the criminally minded. Some of the risks can be managed by the company itself as shown with cyber hygiene and cyber insurance and another takes a collective effort such as community policing but all require awareness of what the particular risks for operating in cyberspace.

These solutions take a variety of investment of either time or money with SMEs, but they are the type of ideas that can help spur interest in alternative concepts to improve the overall risk management. These solutions are somewhat out of the box in terms of using collective power for policing, cyber hygiene to mitigate risk and self-insurance to deal with the accepted risk. Without the awareness and a risk management strategy, it is easy to be swept up by trends an

These three papers mainly fall under the general themes of SMEs collaboratively sharing information in order to better operate in the current environment. SMEs individually will always operate at a disadvantage compared to large enterprises because of the lack of access to budgets and knowledgeable professionals to formulate better policies. However, the collaborative power of SMEs can equalize the playing field in terms or accessing resources and professionals.

This research paper aims to present specific issues that are important towards the overall conversation of cybersecurity and provide reasonable solutions for resolving these problems in the immediate future for SMEs. At first glance, the solutions may appear to be simplistic but if simplification can lead to greater understanding and initiative by the leadership of both sectors to implement changes then it will have proved its usefulness in the policy discussion. There are countless problems with equally countless solutions but if simplification can inspire action to develop a further secure cyberspace. The complexity will never go away, but the systematic approach to solving problems for the major stakeholders will improve the proactive participation and potentially lead to great collaboration to voluntarily build a security framework that works for all.

It also provides an opportunity for policy maker and business leaders to take a step away from the over-reliance on technology to solve all of ones problems. It utilizes seemingly unimportant things such as cooperation, insurance, and active awareness to manage the risk of operating in cyberspace. The consequences for not doing seemingly simple things are much more significant once the surface is scratched. The less obvious take away from these three portfolio papers that while a necessity to present novel concepts to have a greater chance of understanding by leadership. It does not replace the necessity that the leadership have to have buy-in, in order to execute these ideas. The combination of curiosity and education will give leadership an opportunity to incorporate such ideas into improving security on a strategic level.

# PROFESSIONAL RESUME

## EDUCATION

2015 **JOHNS HOPKINS UNIVERSITY | M.A. Government** **WASHINGTON, DC**

- Coursework: Public/Private Management, Federal Contracting Law, Negotiation, International Political Economics, Cybersecurity Policy, and Information Operations.
- Thesis focuses on improving small and medium business cybersecurity through novel solutions such as cyber insurance, cyber hygiene, and community policing in cyberspace.

2007 **AMERICAN UNIVERSITY | B.S. Business Administration** **WASHINGTON, DC**

- Completed university coursework in three years while interning at the following organizations: National Student Partnerships (now known as LIFT), Management Systems International, and the American Electronics Association (now part of TechAmerica.)
- Dean's List.

## WORK EXPERIENCE

2013 – 2014 **STEWARD PARTNERS GLOBAL ADVISORY | Contract Position** **WASHINGTON, DC**

- Established and cultivated working relationships with advisory businesses and financial institutions, ensuring the smooth transition of a $148 million book of high net worth clients brought over from Morgan Stanley.
- Analyzed each household's financial holdings to determine which assets could be transitioned, creating individual transition strategies for the largest households.

2011 – 2013 **MORGAN STANLEY | Financial Advisor** **WASHINGTON, DC**

- Built relationships with wealthy business leaders, resulting in the addition of $13.5 million of assets to the practice and achieving a 92.1% return on those assets.
- Converted $8 million of assets into managed accounts, providing an additional $780 thousand in reoccurring revenue.
- Extended an additional $23 million of available credit to existing clients, whose portfolios previously had not included any lending products.
- Collaborated with a senior partner and other senior executives to develop and implement asset acquisition strategies that resulted sales of an additional $1 million of annuities, $2 million of insurance, $300 thousand of long term care insurance.

- Maintained connections with current and potential investors, including lobbyists, estate lawyers, and executives of major public and private corporations.
- Achieved top tier status within the national Financial Advisor Associate Training Program.

**2007 – 2010** **MORGAN STANLEY SMITH BARNEY | Registered Associate** **WASHINGTON, DC**

- Developed and implemented a strategy to deepen financial relationships with existing clients and to cultivate relationships with new clients, resulting in 10 new clients with $24 million in new assets.
- Systematically analyzed portfolios to identify additional investment, lending, and insurance sales opportunities resulting in the acquisition of an additional $2 million of managed accounts, $6 million of insurance, and a further $1.75 million of refinanced home loans.
- Conducted in-depth market research for strategic business development initiatives.
- Hired, managed, and mentored eight interns over the course of three and a half years, all of whom went onto successful careers at leading investment firms such as Morgan Stanley, Citigroup, and Credit Suisse.

**2006 – 2007** **CITIGROUP SMITH BARNEY | Marketing and Research Intern** **WASHINGTON, DC**

- Structured and updated securities models to track earnings growth, profitability, and valuations of equity positions.
- Analyzed portfolio performance and conducted research on core equity holdings.
- Coordinated recruitment, selection, and training of interns in compliance with hiring guidelines.

## LEARNING EXPERIENCE

**2014 – 2014** **DOKAZI | Co-Founder and Chief Operating Officer** **WASHINGTON, DC**

- Conducted market research to inform the creation of a business plan and marketing strategy for an early-stage technology company that aimed to create an online marketplace to connect data scientists with small and medium sized businesses for short-term projects.
- Conducted research on potential investors and met with venture capitalists, angels, and successful sitting entrepreneurs.
- After further analysis of the existing market situation and financing options, the concept was found to be too nascent to attract necessary number of qualified data scientists and companies with clearly articulated projects requiring such skills.