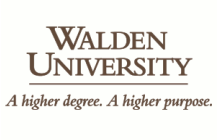

2017

Threat Intelligence in Support of Cyber Situation Awareness

Billy Paul Gilliam
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral dissertation by

Billy Paul Gilliam

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. David Bouvin, Committee Chairperson, Management Faculty
Dr. Godwin Igein, Committee Member, Management Faculty
Dr. Judith Forbes, University Reviewer, Management Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2017

Abstract

Threat Intelligence in Support of Cyber Situation Awareness

by

Billy P. Gilliam

MISM, University of Phoenix 2007

B.S., University of Phoenix, 2005

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

November 2017

Abstract

Despite technological advances in the information security field, attacks by unauthorized individuals and groups continue to penetrate defenses. Due to the rapidly changing environment of the Internet, the appearance of newly developed malicious software or attack techniques accelerates while security professionals continue in a reactive posture with limited time for identifying new threats. The problem addressed in this study was the perceived value of threat intelligence as a proactive process for information security. The purpose of this study was to explore how situation awareness is enhanced by receiving advanced intelligence reports resulting in better decision-making for proper response to security threats. Using a qualitative case study methodology a purposeful sample of 13 information security professionals were individually interviewed and the data analyzed through Nvivo 11 analytical software. The research questions addressed threat intelligence and its impact on the security analyst's cognitive situation awareness. Analysis of the data collected indicated that threat intelligence may enhance the security analyst's situation awareness, as supported in the general literature. In addition, this study showed that the differences in sources or the lack of an intelligence program may have a negative impact on determining the proper security response in a timely manner. The implications for positive social change include providing leaders with greater awareness through threat intelligence of ways to minimize the effects of cyber attacks, which may result in increasing business and consumer confidence in the protection of personal and confidential information.

Threat Intelligence in Support of Cyber Situation Awareness

by

Billy P. Gilliam

MISM, University of Phoenix, 2007

B.S., University of Phoenix, 2005

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

November 2017

Dedication

To my wife, Cindy. Your love, support, and encouragement have been a guiding light during my journey. You sacrificed so much and stood by me in times of success and frustrations, always with words of encouragement. Your prayers gave me the motivation to continue to achieve this goal when many times I was ready to quit. I am truly blessed to have you in my life.

Acknowledgments

I want to acknowledge my dissertation committee: Dr. David Bouvin, Dr. Godwin Igein, and Dr. Judith Forbes. The dissertation committee provided direction, patience, and support throughout the dissertation process. A special acknowledgement to my Dissertation Chair and Mentor, Dr. Bouvin. Your encouragement, advice, and guidance kept me on the right track and instilled in me the motivation and inspiration to keep going, do my best, and achieve my personal goal.

I am also grateful to my family and friends who I did not mention but shared in some way my extraordinary journey. You gave me encouragement when I needed it most, strengthen when I was too tired to continue, and celebrated with me on achieving milestones towards the finish line.

Table of Contents

List of Figures

Chapter 1: Introduction to the Study

Introduction

Technology and security professionals implement various security technologies with the expectation that a certain level of protection is provided against cyber-attacks. Antivirus, firewalls, intrusion detection/prevention, server-based access control lists, and log management software are among the many software and hardware solutions designed to meet this expectation. According to the Computer Security Institute and Federal Bureau of Investigation 2010-2011 computer crime survey report (Richardson, 2010), antivirus and firewalls are at the top of the list for security technologies deployed within the organization. However, even implementing the latest security technology will not in itself protect the organization from attacks. Despite the technological advances in the information security field, attacks by unauthorized individuals and groups have continued to successfully penetrate these defenses. Security technologies such as those mentioned above are designed to detect malicious activity after the event has initiated and in some instances record the penetration process for review by the security analyst at the conclusion of the event, thereby placing the organization in a reactive security posture (AlHogail & Berri, 2012). Reacting to information captured by security technologies does not provide the necessary information for the security professional to fully understand what is important in the defense of the network. Security devices have not always interpreted the data correctly and have provided false positives or recorded false negatives in the security logs.

It is important that the security professional have an awareness of the situations that occur within the network and understand the meaning of the information that is captured and presented by the different security technologies. Situation awareness provides a means to understand what information is important in order to meet the goals and objectives for the security of the network (Endsley, 2012). In the field of information security, situation awareness is dependent on the technological sensors' ability to capture the critical information and to present it for action (Tyworth, Giacobe, Mancuso, & Dancy, 2012). While this concept has been widely adopted in various fields, relying solely on technology and the security professional's ability to maintain a high level of situation awareness in the field of information security is no longer practical in maintaining a sound security posture. With the expansion of global operations through the Internet and the increased complexity in information security in protecting valuable data assets, effective security has become a major challenge for organizations to defend against cyber security threats (Gendron & Rudner, 2012; Hernandez-Ardieta, Tapiador, & Suarez-Tangil, 2013). Security professionals must not only rely on security technologies and their ability to employ situation awareness skills, but must compliment this approach with other security avenues through cyber threat intelligence and cooperative information sharing with partners and allies (Gendron & Rudner, 2012; Fernández-Vázquez, Pastor Acosta, Brown, Reid, & Spirito, 2012). Not only does the security professional need to understand the organization's own security weaknesses in order to improve the defense, but knowledge of the adversary from many different sources is necessary to take an offensive approach in security. By joining technical

innovations and intelligence processes, organizations can counteract cyber threats and gain a competitive edge towards a proactive information security posture (Beer & von Solms Basie, 2013; Sigholm & Bang, 2013). Other avenues are available for sharing information; however, these are at times slow and are available only to a select group of individuals or organizations. In addition, the quality of data may vary over time between sources. Organizations have collected a vast amount of information regarding cyber threats in order to elevate the security posture to a higher level. In a collaborative environment, the sharing of threat intelligence may benefit the security professional by supporting efficient timing of the data as well as providing efficient access to the correct information and its relevance to other organizations.

Background

This study was inspired by the increased cyber-attacks against organizations and the negative consequences that have been experienced as a result of theft of information. In a recent survey of approximately five thousand security professionals world-wide, fifty-three percent stated it is difficult to keep track of the security threat landscape (Ponemon Institute, 2014). As intelligence is essential to the cybersecurity posture, it is also essential to share the information so that countermeasures effective for one organizational environment may be implemented in another organizational environment. This continues to be an important topic as the computing environment and cyberspace continues to evolve in sophistication.

The Industrial and Information Age introduced systems that provided valuable benefits to society. In the Industrial Age, railways and highways offered new and

innovative methods for transporting goods and people across the country. Telecommunications opened new channels to expand commerce and news from local communities to areas across the country and eventually on a global basis. The advent of the Internet and the World Wide Web continued to expand the capabilities of connecting people and industries together without concerns of geographic borders. One of the effects of new systems, whether through railways, highways, or the Internet, is the concept of the network effect. The more people are connected to a network, the more valuable it becomes (Updegrove, 2011). In the 21st century, society has experienced a tremendous growth in benefits and conveniences with technology. Banking transactions, manufacturing order processing, electronic commerce, governments, and connecting to friends and families are just a few benefits of the Internet and technology. As the technology continues to expand and more people are connected, the more the value is increased. From an organizational perspective, the value includes reducing costs, increasing markets, and increasing or improving customer and partner relationships (Farahmand, Navathe, Sharp, & Enslow, 2005; Adeyinka, 2008). Furthermore, organizations are expanding the physical locations globally as technology provides a seamless digital connection for data sharing and reporting and provides a physical presence closer to customers and partners.

With all the benefits and conveniences technology provides, a considerable amount of risk is also present, which if not properly controlled may have adverse consequences. Just as the physical world consists of individuals and groups displaying deviant behavior through criminal acts, the world of the Internet contains the same type

of criminal behavior. The basis for this behavior, or attacks, include acts of greed, financial gain, disruption of organizational progress, or retaliation due to a perceived wrong towards an individual as in employment termination. These attacks have been performed with the backing of foreign governments against another nation in order to disrupt certain government functions or to steal classified information pertaining to a nation's critical infrastructure or more specifically military operational plans (Schneider, 2012). The risks to the organization from these attacks included loss of money, loss of productive time by employees, loss of confidentiality, and loss of reputation (Mendyk-Krajewska & Mazur, 2010; Kim, Jeong, Kim, & So, 2011). As interest and growth of the Internet for business, commercial, and governmental use continues, threats to organizations continue to grow, and network security remains a major concern for organizations worldwide (Adeyinka, 2008). However, the main focus of network security continues to be oriented towards basic security devices that protect the perimeter.

Information security is designed to be a mitigating factor in minimizing security risks (Baker & Wallace, 2007; Conklin & Dietrich, 2008). The focus of organizations in protecting the networks and information from attack is concentrated towards protecting the perimeter and end points. Intrusion detection/protection systems, firewalls, antivirus software, content filtering, and network monitoring systems are conventional security devices designed to add a level of protection against unauthorized access and activities within the organization's network (Kumar & Kumar, 2014). An area of concern with these devices relates to the accuracy in monitoring capability. The rule sets or definition files are constructed by security analysts or administrators to identify the type of attack,

whether it is malware or a direct penetration attempt, based on characteristics that are known. If the characteristics do not match the predefined criteria of the rule set or definition file, the device is unable to accurately identify the attack behavior (Faysel & Haque, 2010). Additionally, this approach towards security is reactive in nature as the devices report activities that have already occurred or are in progress. This diminishes the effectiveness of the security protection. Even with the diminished level of network protection, conventional security technologies are not likely to be abandoned as a security measure as they continue to be effective against limited attacks launched towards organizational networks (Potts, 2012). As attacks continually became more sophisticated, that coupled with reliance on conventional security devices for protection has meant that unauthorized penetration of organizations' networks continued to be successful.

Technology countermeasures have continuously been designed and redesigned to enhance the level of security, but corporations continued to be the victims of successful attacks (Adeyinka, 2008). Even with the available technology to counteract threats for the protection of information and systems and implementing mandatory internal controls, organizational security has not be able to keep abreast of the threats by individuals that consistently arise (Workman, Bommer, and Straub, 2008). New vulnerabilities have constantly been discovered by adversaries, who have developed and launched new exploits to bypass network security devices. The Data Breach Investigation Report for 2012 (Baker et al., 2012) reported that 174 million records were compromised. When combined with the reports for the previous 8 years, over one billion records have been compromised through various methods of attacks. For the year 2011, 98% of the

confirmed breaches were the result of external forces, including organized crime, activist groups, and individuals guided by greed. Interestingly, 81% of the breaches were accomplished through some form of hacking and 69% of these incorporated some form of malicious software.

The threats to information security confronting organizations continually evolve and methods increase in sophistication to remain undetectable to conventional security devices. Viruses and worms transitioned from inconveniences to launching a destructive force that could impact thousands of computers. Computers are being remote controlled through the infection of Bots that employ encrypted communication channels to an external server to receive commands. The attacker may discover and exploit new flaws or vulnerabilities in software without current patches, known as zero-day vulnerabilities, so as to bypass security devices and controls (Koch, Stelte, & Golling, 2012). Attackers have utilized various attack vectors, whether through cyber channels or deception techniques, to gain entry and spread probes throughout organizational technology infrastructure for extended lengths of time in order to meet the main objective of exfiltration of information, a technique known as advanced persistent threat (Brewer, 2014). The motivation of the attacker is no longer fueled by displaying technical skills in subverting authentication and access controls. A primary motivational factor is financially driven by targeting identity theft, corporate proprietary and confidential information, nation-state secrets, and military research and development activities as well as operational plans, to name a few illicit goals (Dlamini, Eloff, & Eloff, 2009; Etsebeth,

2011). Therefore, as each attack yields success and increases the attackers' profitability, the sophistication of new attack methods and frequency continues to increase

Information security professionals are aware of the increased number and sophistication of cyber-attacks against the networks. In an April, 2012, cyber security research report by bit9, Inc. (2012), a survey of 1,861 technology and security professionals indicated that not only have they been aware of the increase in attacks, 71% believed they will be the target of a cyber-attack within the next six months. Specifically, 45% of the surveyed security professionals are most concerned about malicious software and 62% believed anonymous individuals or hacktivists caused these attacks. (Loveland & Lobel, 2011) supported this trend in the Global State of Information Security survey report. PriceWaterhouseCoopers reported that 83% of organizational safeguards were directed towards malicious software based attacks, which represented an increase from 72% the previous year.

Organizations must incorporate a more proactive approach in implementing security controls to meet the security requirements. When attacks occur against an organization's network infrastructure, the security professional must also rely on his situational awareness and the conventional security devices to react appropriately in defense. In other words, the security professional must rely on his knowledge of the current network environment and status (perception), analyze the event (comprehension), understand its potential impact (projection), and determine an appropriate course of action and execute the necessary action (resolution; Miller, 2006; Oliverio, Masakowski, Beck, & Appuswamy, 2007). While maintaining situation awareness provides value to an

organization's information security program, the process still relies on a reactive approach in the defense against attacks. To compliment situation awareness, an early warning system through threat intelligence may add value in incorporating a proactive security program.

Problem Statement

The attempted penetration of security defenses is recorded in the system event logs providing the security analyst with capability to identify the attempt to breach the network (Ponemon Institute, 2012). The reliance on logs have not provided the necessary information to comprehend certain actions at the time they have occurred as the devices only generated alerts for known signatures. Some breaches in defenses have been conducted in a slow penetration method that was undetectable and did not alert the administrator. Because attack methods and the computing environment constantly change, the reliance on a predetermined set of actions have derived inconclusive or misleading results.(Yang, Byers, Holsopple, Argauer, & Fava, 2008). Utilizing shared threat intelligence between organizations is increasing, but also a lack of research indicating whether the organization has received any value through the shared process in order to maintain a proactive security approach.

Purpose of the Study

Information security is in need of a change from reactive to proactive defense and must include the ability to understand the motives of the attacker as well as the tools and methods used in attacks. Advanced knowledge of unusual patterns that provide evidence of an attack, a specific system and/or process toward which the attack is directed, or the

types of information that are the target of the attack may improve the organization's ability to proactively increase security measures where necessary. Intelligence through the sharing of information between organizations may provide the advantage of shifting from reacting to an ongoing attack to becoming proactive in understanding the threat, intent, and motives of the attacker in order to reduce the likelihood of a successful attack (Hutchins, Cloppert, & Amin, 2011).

Little research has been offered to identify the value of available shared information through threat intelligence as the information that is necessary for the security professional or decision-maker to make a qualified decision (Tadda, 2008). The purpose of this study was to explore whether the value of current threat intelligence increased the security analyst and decision maker's situation awareness so as to proactively detect a potential adversary's intention.

Nature of the Study

The nature of this study was to understand the value threat intelligence provided to the security analyst's and decision maker's situation awareness so as to minimize or prevent the consequences of an attack against the organization's information and network security.

The increased speed and sophistication of how attackers exploit vulnerabilities necessitates the need to support decisions in response in the shortest amount of time possible. Several databases are available to identify previous types of attacks and mitigated solutions including the National Vulnerability Database, Common Attack Pattern Enumeration and Classification, and Common Vulnerabilities and Exposure.

These avenues provided important and relevant information, but lack of timeliness of the information is a growing concern. In a recent study on sharing cyber threat intelligence (Ponemon Institute, 2015), 47% of 692 respondents experienced a significant security breach compromising enterprise systems. Most respondents (65%) stated that threat intelligence could have prevented or minimized the impact of the attack. While some concern remains regarding trust in sharing information, a growing recognition exists that the sharing of threat intelligence may lead to improving an organization's security posture and situation awareness. Threat intelligence is designed to provide and distribute solutions to threats against an organization's computing environment as expeditiously as possible, thereby minimizing the consequences of the attack and decreasing the time between the vulnerability being discovered and mitigating actions against the threat being initiated.

I conducted a case study in order to determine whether situational awareness complimented with threat intelligence resources provided the security professional with the ability to proactively identify attacks, resulting in the proper execution of countermeasures to reduce or eliminate the threat impact. A case study was the methodological design the most appropriate for research for this topic, as it provided for research on a specific issue through one or more cases that was bounded by a setting or context (Yin, 2009). The participants in the research study were security professionals currently actively participating in the security of an organization.

Research Questions

Based on the methodology of case study research, this research addressed the main question of how important threat intelligence is in supporting situation awareness for the security analyst and the decision maker. Specifically, the questions this study was designed to answer were:

RQ1: How effective is situation awareness in response to cyber-attacks?

RQ2: How does threat intelligence support situation awareness in response to cyber-attacks?

RQ3: How difficult is maintaining situation awareness for information security?

RQ4: What effect on information security was due to the combination of threat intelligence and situation awareness?

RQ5: Why was implementing threat intelligence with situation awareness successful or unsuccessful in the goal of information security?

Conceptual Base

Three conceptual bases were used for this research study. The first conceptual base for this study was Boyd's theory of Observe-Orient-Decide-Act (OODA) loop in the decision-making process (Boyd, 1987a). According to Boyd's theory, to gain the advantage over an adversary, an individual must process the loop at a faster rate than the opponent so as to create confusion and chaos and prohibit the ability to generate an effective situation awareness. A second conceptual base was Endsley's situation awareness process for decision-making in dynamic systems (Endsley, 1994). Situation awareness is an extension of Boyd's "Orient" and "Observation" phase and is the process

of perceiving the elements in the environment, comprehending their meaning as compared to the individual's mental models and how they relates to the goal, and projecting the impact the elements have in the future. While situation awareness originated in the aerospace field, the concepts have been adopted to other fields, including systems that are dynamic in nature. In the field of cybersecurity, change occurs at a more rapid pace. In the OODA loop and situation awareness, time may be measured in minutes, hours, or days. However, in the realm of cyberspace, change may occur at the speed of light. The third conceptual base was Barford's realm of cyberspace. Due to the dynamic nature of cyberspace, Barford, et.al (2010) expanded the concept of Endsley's (1995, 2012) situation awareness towards understanding the behavior and intentions of the adversary within the realm of cyberspace. An understanding of the adversary's intent, opportunity, and capability in addition to knowledge of the vulnerabilities within the environment is necessary to adequately project the future situation. I discuss the theories of Boyd, Endsley, and Barford in more detail in Chapter 2.

Definition of Terms

Attack: A deliberate act by an individual or group to gain unauthorized access to a network or system or to prevent authorized users from utilizing the network resources (Cole, 2011).

Cyber intelligence: Tracking the capabilities, intentions, and activities of potential adversaries as they evolve within the cyber domain; collecting and analyzing the information in order to produce timely reports in support of the decision-maker (Mattern, Felker, Borum, & Bamford, 2014).

Intrusion: An attack on information systems and assets in which the adversary attempts to gain entry or disrupt the normal operations with the intention to do malicious harm (Whitman & Mattord, 2010).

Mental model: A cognitive process to gain an understanding of how something works that assists in determining what information is important. Without a mental model, it is difficult to understand what is happening and what may happen in the future (Endsley, 2012).

Security: The set of principles, methodologies, tools, and techniques that protect the confidentiality, integrity, and availability of network devices and information (AlHogail & Berri, 2012).

Security controls: The countermeasures (management, operational, technical) designed to protect the security of systems and information (U.S. Department of Commerce, National Institute of Standards and Technology, 2006).

Virus: Self-replicating programs that infect and propagate through files and infect systems and/or boot-records. This may occur by attaching to files the user does not see (Adeyinka, 2008).

Vulnerability: A weakness in a system allowing unauthorized actions. The weakness may be a result of design flaws, implementation errors, or configuration errors (Bosworth, Kabay, & Whyne, 2012).

Zero-day exploit: A flaw in software that is discovered and a program exploiting the flaw is available before the vendor is aware of the flaw (Koch et al., 2012).

Assumptions

For this research study I assumed that the best data was available through case studies of organizations that have dedicated security professionals and that the information was relevant to the study. The second assumption was that the security professionals interviewed were truthful and provided unbiased information. The third assumption was that the data was collected in a timely manner. The fourth assumption was that the security professionals provided the knowledge relevant to their professional experiences. The fifth assumption was that the participants experienced an attack against the organization's network. Without open and accurate information, understanding the value of intelligence for the organization would have been difficult to determine.

Limitations

The limitations of the study were based on the availability of the data to support the research. Little control was exercised on whether any individuals participating in the research provided the critical and relevant data. While some information was offered, reluctance to disclose certain information was evident when addressing information and network security. The research required individual participation without compensation and did not guarantee that the participants would allocate time throughout the research. It was possible to obtain data from other research organizations; however, no guarantee was offered that the specific data needed for this research topic would be complete or entirely relevant.

Delimitations

The selected participants were security professionals representing various organizations. The participants were required to be in a role or position that provided them with direct contact during an attack, and the participants were required to have first-hand experience with an attack towards the security posture, regardless of whether the attack was successful. I did not consider any respondent without these requirements for this study.

Significance of the Study

Technology is a major facilitator in every aspect of society, from economics and social interactions to professional and government functions (Bosworth et al., 2012). People have learned to rely on the speed of computers and the universal connectivity through the Internet in which activities can be accomplished in seconds without the concerns of geographical boundaries. Individuals communicate through electronic mail and instant messages, conduct financial transactions, and search the Internet for information. Organizations conduct various types of business from e-commerce to confidential business proposals through the Internet. Data is archived in computers ranging from individual personal information to past financial records, either due to regulatory requirements or based on the organization's business model. In essence, computers connected to the Internet have evolved not only as a benefit, but as a necessity.

With all the benefits and conveniences technology has to offer, the opposite is a dark side of implementing technology. Just as financial institutions encountered crimes by robbers and automobile owners encountered crimes by thieves, it is not surprising that

computer users and the Internet have encountered cybercrimes. While technology countermeasures have been continuously designed and redesigned to offset these attacks, corporations continued to be the victims of successful attacks. Research indicated that security professionals exercised elements of situation awareness to comprehend the security changes within the environment and projected the impact as it related to the goal of information security (Cyril, 2012). As the cyber environment continued to change at a rapid pace and new attack methods were being implemented, the process of situation awareness has not allowed the security professional to function in a proactive state (Jajodia, Liu, Swarup, & Wang, 2009). Through the implementation of threat intelligence as an added process to situation awareness, the security professional may be able to understand the threat and impact on the network and may plan the necessary countermeasures to minimize any future consequences.

The positive social change resulting from this research is that it may benefit several groups. One group is the security professional responsible for implementing countermeasures. Through an understanding of the issues and consequences as a result of advance threat intelligence in the decision process, security professionals may modify the risk assessment methodology so more accurate analysis may be performed. Another group receiving benefit is corporate management. Through the accurate analysis of risk by the security professional and the potential consequences facing the organization, external influences in the decision process may be modified to provide more support. This support may be in the form of active participation by management, increased

personnel for proper staffing, increased funds for implementation, and targeted training for increasing expertise in the area of information security.

Summary

Due to the dynamics of cyberspace, security personnel have been faced with relying on technology in addition to individual situation awareness ability to identify attacks while faced with the challenge of identifying new methods of attacks and understanding the significance in relation to the goals of information security. Threat intelligence offers security professionals valuable information to complement their situation awareness and implement a proactive posture to defend against adversaries and the attack methods. The research study was based on the theoretical concepts of Boyd, Endsley, and Barford. Based on these concepts, in this research I examined the effects of incorporating a threat intelligence model with situation awareness. The expectation derived from this study was to gain a better understanding of whether threat intelligence has a significant effect on information security so that new models may be defined.

Chapter 2 provides a literature review of past and current literature and research to support that current security technologies and situation awareness have diminished in effectiveness for proactive measures in protecting information. Chapter 3 details the research design and methodology for this study.

Chapter 2: Literature Review

Introduction

This chapter presents the approach to researching the literature pertaining to the difficulties in information security defense based on technology and the cognitive abilities of situation awareness by the security professional. To be more proactive in security, threat intelligence may provide the professional the advance information required to minimize or eliminate consequences of the threat. The first section of this chapter presents the searches, terms, and resources performed for this review. The next section provides the background and definition for information security. In the next section, I offer an overview of network attacks and with the continued reliance in computers and discuss the increased sophistication of attacks against organizations' networks. The next section provides the theory of Boyd's OODA loop and the benefit the theory has in confronting an adversary. The next section provides the theory of Endsley's situation awareness and its relation to Boyd's OODA loop. Next, I discuss cyberspace and the challenges in providing security. The final section presents cyber threat intelligence and the value advance information relating to an attack may provide the professional with a proactive approach to security.

Search Strategy

The literature search strategy included the utilization of several databases of academic periodicals, journals, and peer reviewed technical papers through selected key word searches. The key words included *situation awareness, situational awareness, security, information security, network security, computer security, cyber security, cyber*

threat, cyber-attack, Internet attack, cybercrime, intelligence, counterintelligence, hacker, attacker, intrusion detection, human computer interface, information sharing, knowledge sharing, malware, Advanced Persistent Threat, critical infrastructure, and *detection.* Academic articles were searched through Walden University Library: ProQuest Central, Academic Search Complete, EBSCOhost, Science Direct, Computers and Applied Sciences, Institute of Electrical and Electronic Engineering digital database, and Association of Computing Machinery digital database. I utilized Google Scholar search engine to retrieve relevant articles from multiple online databases. I used the dissertation database through Walden University, and the search included all published dissertations within the past 5 years from all universities. I accessed local university libraries (Washington University in St. Louis, Missouri and Southwestern Illinois College in Belleville, Illinois) through personal visits to conduct additional research. In addition, I queried government and government sponsored databases to include National Institute of Science and Technology, United States Secret Service National Threat Assessment Center, and the Computer Emergency Response Team Coordination Center of Carnegie Mellon University.

I reviewed books, both online and print, for background and historical information specifically relating to this study. Newer editions (within the past 5 years) were a source for the latest developments significant to the study. I reviewed newspaper articles and industry specific electronic newsletters to keep abreast of information security and cyber-attack topics, but I did not include them as part of the literature

review. The value gained from these periodicals was the identification of new key words for search purposes.

Situation awareness is not only relevant to computers and networks but has its roots in the military environment. Articles pertaining to military pilots and ground forces were reviewed to gain an understanding of the origin, concepts, and practical application of situation awareness. For relevant historical purposes, articles were included that were published over the past 25 years. While the concept of situation awareness has been extended to other fields, many of these were not significant to the study of information security. The transition from situation awareness to the field of cyber situation awareness is a relatively new field of study; therefore, relevant articles and studies have primarily been published within the past 5 years.

Literature Review

Technology is a major facilitator in every aspect of society, from economics and social interactions to professional and government functions. People have learned to rely on the speed of computers and the universal connectivity through the Internet in which activities can be accomplished in seconds without the concerns of geographical boundaries (Bosworth et al., 2012). Organizations conduct various types of business, from e-commerce to confidential business proposals through the Internet. Data ranging from individual personal information to past financial records is archived in computers due to regulatory requirements or based on the organization's business model. In essence, computers connected to the Internet have evolved not only as a benefit, but also as a necessity. An analysis of Information and Communication Technology for 159 countries

has shown a positive effect and played a vital role in economic growth (Farhadi, Ismail, & Fooladi, 2012). As organizations expand and increase in competitiveness in the global market, reliance on computing technology has increased (Chu, 2013; Farahmand et al., 2005). It is not surprising that information is one of the most important assets for any organization. As computers and their related technology expands and improves, so does the importance of the information to the organization. Confidential and proprietary data, patents, contracts, and business strategic plans are critical business assets contained in computer systems. Executives in organizations base decisions on the reliability, accuracy and speed of availability to the information when needed. The absence of these qualities may, and most often does, have a negative impact on the organization, including jeopardizing its existence (Etsebeth, 2011). The protection of information assets is vital through effective practices and relevant technologies regarding information security.

Information Security

Information security as defined by the International Standards Organization is the "preservation of confidentiality, integrity and availability of information." In addition, the International Standards Organization defines an information security event as "an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant" (International Organization for Standardization, International Electrotechnical Commission, 2005, p. 2). To meet these objectives, the organization must implement countermeasures and evaluate whether these controls are effective in protecting the organization from network breaches or attacks.

In the 1980s, personal computers became widely available and individuals began to increase their knowledge of computers and applications. Even though the personal computer was a standalone desktop computer, these devices were capable of performing word processing and financial calculations. Organizations began to utilize this technology for automating manual processes. However, while this approach was more efficient and convenient for the worker, it was difficult to share information with others (Bosworth et al., 2012; Whitman & Mattord, 2010). To add more value to the organization and increase productivity and efficiency, users required the ability to communicate and share information with other users.

In the 1990s, with the advancement of technology, personal computers became more powerful and organizations began interconnecting the computers through local area networks (LANs). Not only could users share the information, but LANs also provided connectivity to mainframes, downloading data, and executing programs at the workstations. By the end of the 1990s, the growing popularity of networks enhanced the development of methods to expand the connectivity into wide area networks (WANs). This provided the means for users and computing devices to interconnect across a wider geographical area.

The Internet began as a Department of Defense communication project known as ARPANET. The project was divided into two parts, one for research (ARPANET) and one for military use (MILPART) and was designed to demonstrate the ability for packet switching within the military command and control system. The project was a success and in 1989, the ARPANET portion of the project was shutdown (Lukasik, 2011). In

1990, T. Berners-Lee introduced a new and expanded method of computing known as the World Wide Web (Bosworth et al., 2012). The capability of the World Wide Web allowed users and organizations to expand access to information within the global community. Initially, the government controlled the Internet and restricted its use to government agencies and government contractors. However, during the 1990s the government released its control resulting in an immense system of interconnected networks. This explosion provided an enormous opportunity for organizations to compete on a global basis without the geographical boundaries.

Network Attacks

As businesses, governments, and society have become dependent on computer networks, information processing ranging from banking transactions to critical infrastructure relied on information technology solutions through the use of the Internet (Jang-Jaccard & Nepal, 2014). With the growth and dependency of computers, attacks began as a benign form of intrusions through malicious software. Viruses mainly displayed a message on the user's screen and were not harmful to the computer or data (Dlamini et al., 2009). However, malicious software has evolved to the point that destruction of systems and data can be achieved.

Workman et al. (2008) argued that organizations continued to be adversely affected through information security vulnerabilities. Even with the available technology to counteract threats for the protection of information and systems and implementing mandatory internal controls, organizational security has not be able to keep abreast of the threats by individuals that consistently arise. While automated procedures using

specialized technologies are known to improve the information security posture coupled with the publicity of security vulnerabilities to inform the public of the security threats, security professionals have frequently failed to understand the significance of the threat at the time it is discovered. To address this problem adequately, it is imperative that an understanding of the process used by the security professionals in deciding whether to implement certain security precautions be attained. Several factors may be responsible in the decision process, for example, lack of adequate resources, lack of adequate training or practical experience). Another potential factor is that security professionals and managers do not know what measures to apply, when to apply them, or why these measures should be applied (Workman et al., 2008).

From the attacker's point of view, not all computer systems are created equally and each have different levels of complexity. The popularity of the systems and software have a direct relationship to the attack level and frequency. Since Microsoft is very popular in the corporate environment, it is not surprising that it is the system that is attacked the most (Jumratjaroenvanit & Teng-amnuay, 2008). Investigating these areas of vulnerabilities and the methods that are used by hackers are designed to provide security professionals methodologies for implementing security best practices in the organization's computing environment. However, successful attacks continue to be carried out through methods that are already known.

The challenge related to information security is the complexity of the network and the rapid growth and expansion to remain competitive in the global market. Businesses continue to increase reliance on technology in all industries, including financial,

manufacturing, government, and electronic commerce. A result of this increased reliance is the rise in activities of cybercriminals. In 2011, the second highest level of compromised data records were reported since 2004, a major increase over 2010: 174 million records compared to four million records respectively (Baker et al., 2012). For the previous 8 years, one billion records have been compromised by cybercriminals. This increase has led to an understanding of the importance of designing and implementing proper security controls (Conklin & Dietrich, 2008).

OODA Loop

The OODA Loop is a decision cycle in which the decision-maker interacts with the environment through four steps and is able to adapt, or change based on feedback during the process in order to achieve a desired state or goal. John Boyd provided the basis for this concept in his theory "Destruction and Creation" (Boyd, 1987a) by outlining how individuals "comprehend and cope with our environment" in order to develop mental concepts or maps. Individuals create and destroy these mental images based on the changing environment to match reality and is able to "survive on our own terms" (Boyd, 1987a). Boyd's theory was developed through his research to explain why American fighter pilots during the Korean War were able to out maneuver and be more successful than his adversary. Boyd determined that part of the success was based on the F-86 Sabre fighter jet's bubble-shaped canopy, increasing the ability of the American pilot to observe, orient, decide, and act (OODA) more quickly than his adversary's Chinese MiG 15 fighter jet (Boyd, Richards, Spinney, & Richards, 2007; Bryant, 2006; Polk, 2000). The OODA Loop is part of Boyd's expansion of the characteristics of fast

transients in conflict. The idea of fast transient indicates that in order to win, one must operate at a faster rate or rhythm than the opponent so as to make one appear unpredictable and create confusion and disorder among the adversary (Boyd, Richards, Spinney, & Richards, 2007). Concepts of meaning were developed to represent our perceived reality. Boyd described this process through the concept of creative induction, which brings order and reason to reality. When the creative induction process is disrupted in such a manner that the perceived reality changes, the result is destructive deduction or, in other words disorder and chaos (Boyd, 1987a; Polk, 2000). To achieve the characteristics of fast transient, Boyd states that the opponent must get inside the adversary's decision-making process of observation-orientation-decision-action loop so they are not able to generate mental images fast enough that agree with the patterns of conflict (Boyd et al., 2007). Boyd's theory combined the physical (current state of the environment), with the cognitive (mental maps and concepts) in order to achieve a specific goal, which was to survive on one's own terms and to improve the capacity of independent action while denying the opponent the same goal in a military conflict (Boyd, 1987c). To achieve this goal, it was also important for the opponent to process the loop at a faster rate than the adversary.

The OODA loop is initiated through the process of observing the environment by the decision-maker through acquiring information through various sensors. These sensors, which may be physical (eyes, ears, smell, touch) or through other devices (video, camera) allow the decision-maker to collect information that aids in understanding the

current state of the environment and aids in forming a mental concept, or mental map, of the environment. As new information is obtained, it is analyzed in the Orient phase.

Orientation phase was considered by Boyd to be the most important phase of the loop. It is the key process that ties the others together and is described as the *schwerpunkt*, or the focus of the main effort. Boyd states "Orientation is the *Schwerpunkt*. It shapes the way we interact with the environment – hence orientation shapes the way we observe, the way we decide, the way we act." (Boyd, 1987b). During the orient phase, the decision-maker interprets the new information in relation to the existing knowledge of the environment before adjusting the new mental map to depict the updated state of the environment. The interpretation of the information is based on the individual's cultural traditions, genetic heritage, previous experiences, new information, changing or unfolding circumstances, and analysis. (Boyd, 1996; Brumley, Kopp, & Korb, 2006; Hammond, 2013). Once the new mental map or current state of the environment is formulated, the individual can decide the appropriate action.

The decide phase uses the new mental map to process different hypotheses about the situation and what actions to take in response. With the new mental map of the environment, the individual has a better understanding of how the actions will impact the future state and whether the result will be a positive or negative consequence of the decision. Upon determining the action that offers the most positive consequence, the individual performs the action.

In the action phase, the manipulation of the objects in the environment occur which results in changes. If the action was based on a rational decision-making process,

then the existing state of the environment may change to maximize the positive consequence and minimize the negative. This change is observable by the individual as well as others and generates a new observable state of the environment. The OODA loop was designed to be a feedback process between the individual and the environment. Since actions alter the current state, as new information is gained, hypotheses are considered and action taken, feedback is iterated through the loop.

Boyd's work was based on the strategies and tactical methods of aerial combat. While his influence and contribution to aerial combat and aircraft design is widely regarded, Boyd's work as a strategist, especially the OODA loop, is a topic of controversy (Hasík, 2013). Critics contend that part of the challenge in accepting his ideas centers in the difficulty of defining what his theory represents and whether it is called Boyd's Theory (military strategy) or the OODA Loop (decision-making process). For some, it is the OODA Loop that describes the human cycle of decision-making while others describe it as a command and control process. Others regard his ideas as a theory of warfare (Polk, 2000; Samuels, 2014). In addition, controversy was founded in Boyd's lack of scientific testing and academic publication. While his experience as a fighter pilot influenced his theories, Boyd did not publish any of his works or seek out any peer reviews for validity. His work does not contain any hypothesis and test results nor does his work contain any scholarly references to support his arguments (Osinga, 2013; Polk, 2000). Instead, he presented his theories in a series of oral slide presentations supported by his own experiences as a fighter pilot, his studies of other military theoreticians, including Carl Von Clausewitz, Alfred Mahan, Giulio Douhet, and his in-depth review of

military history coupled with social and physical sciences (Hasík, 2013; Mets, 2004). Boyd often stated that victors were victorious because they operated inside the opponent's decision cycles. However, he did not model any variables or processes within the OODA loop to support his position. Grant and Kooter (Grant & Kooter, 2005) argued several shortcomings exists in the OODA process. First, Boyd did not specify the overall scope of the four stages in the process or attempt to decompose any of the stages other than orient. As an example, the process does not offer sub-divisions to determine how the decision-maker interprets the new information as compared with the original concept or mental map of the environment. Also, as a result of the act phase, the process does not identify the steps required to determine whether the result of the act was successful. Second, the process displays shortcomings in that it lacks memory and attention, and cognitive representations of world states or deliberate planning processes. Third, the process does not model any interaction of the loop with the adversary, which would impact the feedback loop of the process (Grant & Kooter, 2005; Hasík, 2013). Sub-processes are missing from Boyd's presentations of the OODA Loop, however no evidence exist that indicate these processes were not presented in oral fashion.

Many of the published critiques of Boyd's work are based on the ideas from different perspectives of the interpreters. Since Boyd did not publish his work but presented oral briefings, these interpretations were derived not from the participation in his briefing, but from examining the slide presentations of *Discourse on Winning and Losing*, *Organic Design for Command and Control*, *The Strategic Game of ? and ?*, *The Essence of Winning and Losing*, and *Patterns of Conflict*. In order to properly analyze

and interpret Boyd's ideas, one would need to review over 300 slides and be conversant in the areas of social science, military history, and science and technology so as to place them in proper context (Hammond, 2013). For example, one of the most recognized concepts of Boyd's OODA loop is the wheel of four arrows labelled Observation, Orientation, Decision, and Action. The OODA loop completes one phase then connects to the next phase in a circular pattern.

While this diagram is most often used in association with his ideas, this simplistic view was never drawn by Boyd. The process is more complex with available feedback and feedforward loops contained in each phase, making each phase an interrelated process (Philp & Martin, 2009).

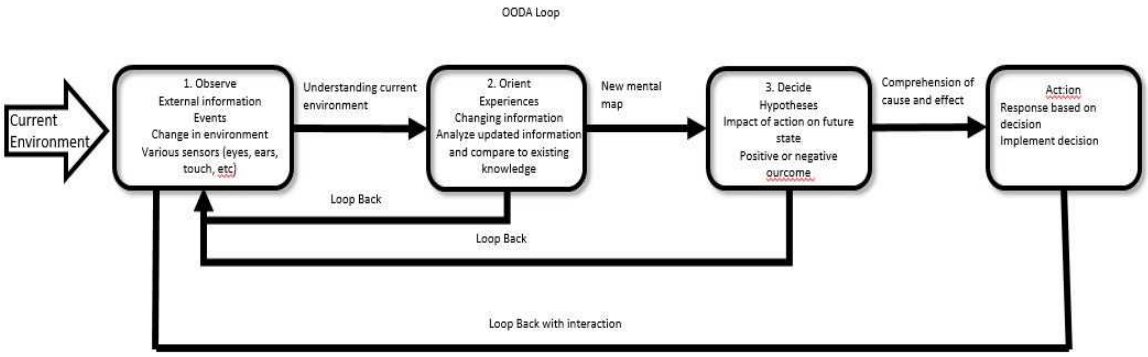

Figure 1: Boyd's OODA Loop

Boyd developed his theory in relation to war and contrary to many of his critics was not intended to be more than an outline or guide to act according to the changing environment. While his OODA loop process can be further presented in more detail at each process, Boyd was more interested in presenting the human behavior and decision-making process while having his audience think "outside the box". As Hammond argued,

Boyd's style was interrogative and focused more on questions than answers in order to find new methods to solve problems. Effective decision-making requires the decision-maker to be aware of the current environment and examine the unforeseen and changing situations from various perspectives so that the individual's mental model or image can adapt to correspond with the changes. Through the mental processing of updated information the decision-maker is able to decide on the most appropriate response and act on the decision.

OODA and Situation Awareness

Boyd's OODA loop model originated as a representation of the decision-making process within the military and has since been expanded to other areas, especially where a competitor is trying to gain the advantage over an opponent (Marra & McNeil, 2013). The ability of the decision-maker to assess, or be aware of the current environment and make adjustments at a faster rate than the opponent as the situation changes is a major factor in the quality of the decision process. As in Boyd's OODA loop, the perception of the current environment as observed through senses or displays is the foundation for concepts of situation awareness in the decision-making process. However, situation awareness involves more than receiving various pieces of data. It is necessary to gain a level of understanding of the situation, comprehend its meaning, and the ability to project future states of the system in accordance with the operator's goals. Situation awareness is described as a detailed description of observe and orient stage of Boyd's OODA loop model and a key component in the decision-making process (M. Endsley & Jones, 1997; Salfinger, Retschitzegger, & Schwinger, 2013). Endsley provides the detailed sub-

process that compliments Boyd's OODA Loop through the identification of perception, comprehension, and projection.

Situation awareness has its foundation in the study of pilots' ability to maintain awareness of the different complex and changing events that occur during flight and how this information is used to predict future actions. While several definitions appear in literature, it is Mica Endsley's seminal work and formal definition that has been widely adapted, not only in the field of aviation, but has expanded across multiple fields of study (Tenney & Pew, 2006; Wickens, 2008). Endsley defines situation awareness as "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" (Endsley, 1988a). In other words, it is the internal model of the world around him (pilot) at any point in time (Endsley, 1988b) and being aware of what is going on in the current environment, being able to discern what is important, understanding what these factors mean in relation to the goal, and what will happen in the near future (M. Endsley & Jones, 1997; Onwubiko, 2009). Since Endsley's original research, various definitions have been presented to support situation awareness in the decision-making process: the continuous perception of self and aircraft in relation to the dynamic environment (Carroll, 1992); responding to informational cues based on humans, important information, behavior, and appropriateness of responses (Dalrymple & Schiflett, 1997); the integration of knowledge that results from recurring assessments (Sarter & Woods, 1991); a cognitive understanding of the current situation and its implications (Vidulich, 1995). The common element of the various definitions convey the point that situation awareness

is a cognitive process that represents an individual's perception of the elements within the environment and is supported through external sources including visual displays, senses, or relevant information from other individuals in order to determine the appropriate action in the decision-making process. Situation awareness, however is not an automated system, technical device, or external display, but a state of human awareness based on a level of understanding the situation, comprehending the meaning, and the ability to project the future state of the environment in accordance with the goal of the individual (Endsley, 1994; Lambert, 2001). Based on Endsley's formal definition, situation awareness was developed into three levels, or stages of understanding, each built upon the other.

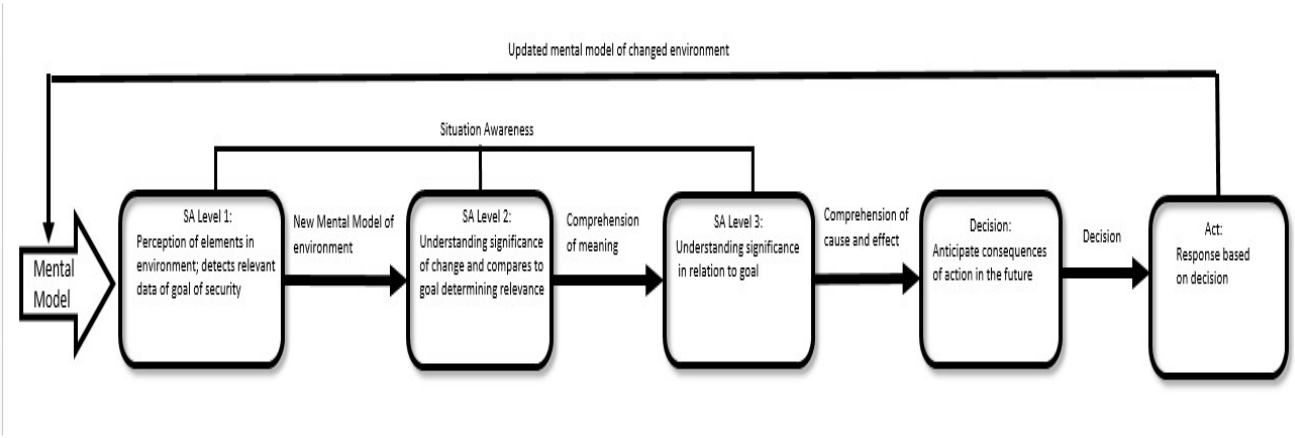

Figure 2 Model of situation awareness process.

Level 1: Perception. Level one is the perception of the elements of the environment. The perception is knowing the important elements of the computing environment, including the relevant attributes, status, as well as the overall dynamics (Endsley, 1994; Mihailovic et al., 2009). Perception across different domains are different and each will contain different characteristics and dynamics. For example, a

physician may use his or her senses and available information in assessing the health of the patient and detect subtle differences. An automotive mechanic may detect abnormal conditions of an engine based on the sounds or devices designed to monitor engine performance. In complex information systems, much attention is directed towards the use of electronic displays and various reports that directly perceive the status of the environment (Endsley, 2012). Within information and network security, the challenge in attaining accurate perception is detecting all of the relevant data and disregarding data that is not relevant to the goal of maintaining and securing the network. The operator needs to maintain an awareness of the status of the computing environment by relating to the various devices and services that comprise the computing environment as well as the activities conducted by individuals using the services of the network. The security analyst perceives the various data on the status of the network firewalls, routers, switches, intrusion detection/prevention systems, servers, and network storage devices, as well as the real-time data traffic traversing the network. The data, referred to events in this context, report various activities across the network and its devices. Events may include activities such as normal logons by authorized users, incorrect password attempts, amount of data transferred from one device to another, network interrogation by outside sources, and network services started or stopped. The security analyst must sort through this information in order to gain a proper understanding of the current environment. A vast amount of data is being presented that is competing for the attention of the operator or analyst and as a result, the potential for failure to accurately perceive the environment is great (Endsley, 2001; 2012). According to Endsley's model, the perception of the

current environment is stored in a mental model which is a representation of the static knowledge of the environment (Endsley, 2000). Without an accurate mental model of the current environment and important information, the individual is at risk of not detecting changes as they occur within the environment, and form an incomplete or inaccurate representation of the new environment (Endsley, 2000; Rosli, Rahma, & Alias, 2011). An inaccurate representation of the environment may inhibit understanding the impact to the security goals and objectives necessary to achieve level two of situation awareness.

Level 2: Comprehension. Comprehension is more than just being aware of the elements and status of the environment. It is gaining an understanding of the significance of the elements and compares this information to the goals and objectives as supported by the new mental model of the environment. In other words, perception of the elements gained in Level One, combined with comprehension of the meaning to form patterns of the fragmented information provides a complete mental picture of the environment and the significance of its meaning based on combining new information with existing knowledge (Salerno, Hinman, Boulware, & Bello, 2003). Comprehension is compared to the goals and objectives of the environment to determine its relevance in attaining the goals (Endsley, 1995, 2001, 2012). For example, a physician assesses the health of a patient through exams and external devices. The information gathered at this stage may not provide any significant details. However, through his expertise and experience he is able to combine the various pieces of information and comprehend the meaning as to whether the patient is healthy or treatment is necessary to achieve the overall goal of a healthy patient. Likewise, the security analyst goals in information security include

maintaining confidentiality, integrity, and availability of the information and the computer systems (von Solms & van Niekerk, 2013.; National Institute of Science and Technology, 2006). For the analyst to achieve comprehension, he must not only be aware of the data provided by the security devices, system logs, and monitoring software, but must comprehend the significance of the data as it relates to the protection of the confidentiality, integrity, and availability of the information.

Errors within the process of situation awareness occurs in the comprehension phase. In the case of errors, the individual receives the necessary information relating to the status and elements of the environment, however due to lack of experience is not able to comprehend the meaning in relation to the goals. For example, the security analyst has gathered information from the various security devices and software. Due to lack of experience in the security field and knowledge base, the analyst is not able to comprehend the meaning of the various pieces of information and is not aware the network is experiencing a low-level attack. Because the analyst does not have a good knowledge base of previous experiences, he is at a disadvantage in adequately attaining and developing level two situation awareness.

Level 3: Projection. Level Three is the highest level of situational awareness and is the ability to project the events that will occur in the future (Endsley, 2001;Luokkala & Virrantaus, 2014). Projection is achieved through the perception of events occurring within the environment and gaining an understanding of the cause and effect in relation to the overall goal so that the decision maker can anticipate the effects and devise a course of action. To achieve this level, it is important for the decision maker to have a good

understanding of the domain and the expertise to understand the operations and dynamics of the system. This, in turn, supports the ability to gain insight into the meaning of the information provided (Level 2) and its relation to the goals in order to project the future actions of the event (Endsley, 2012; Luokkala & Virrantaus, 2014). Through this process, a plan of action may be formalized that support the goals of the decision maker in a timely manner.

Situation awareness is comprised of two distinctive processes: technical and cognitive. Technically, situation awareness is acquiring, compiling, processing and fusing different pieces of information. Cognitively, the decision-maker must be able to evaluate the different pieces of information, determine its relevancy or quality, and understand its implications in order to comprehend the implication so an informed decision or course of action may be pursued in relation to the goal. As indicated in the formal definition by Endsley, situation awareness is a progressive process with each level increasing the individual's awareness resulting in the ability to predict future actions.

Situation Awareness in Cyberspace

The physical world is defined by four distinct domains, each with geographic boundaries and measurements comprising of land, sea, aerospace, and space. Geographic boundaries may include regions or countries as well as defined sovereign rights for national security purposes. Boundaries may be reduced in size, such as the visual limitations of an individual when observing the immediate physical world around him. Measurement for distance is defined by feet and miles while time is measured in minutes, hours and days. The elements of boundaries, measurements, and time shape the

mental model of the current environment for the individual. As changes are perceived by the individual through visual displays or senses, the individual comprehends the significance of these changes and projects the future impact. The individual is then able to determine the appropriate action. This process of situation awareness within the physical world has been studied and applied in different fields to include military operations, aviation, critical infrastructure systems, automotive, and healthcare. Since the beginning of the 21st century, researchers have shown a growing interest in the application of situation awareness to the realm of cyberspace, which is described as the fifth domain along with land, sea, aerospace, and space.

The term cyberspace was first defined by William Gibson in the novel "Neuromancer" as "a consensual hallucination" or "an artificially created perception or vision that is common to a community of users" (Gibson, 1984). Since the 1980s, several definitions have emerged to formally define cyberspace. Cyberspace is "distinct entities with clearly defined electronic borders" (Schwartau, 1994); "the confluence of cooperative networks of computers, information systems and telecommunication infrastructures commonly referred to as the Internet and the World Wide Web" (Sharp, 1999); "a physical domain resulting from the creation of information systems and networks that enable electronic interactions to take place" (Rattray, 2001). The Joint Chiefs of Staff defined cyberspace as "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange information via networked information systems and physical infrastructures" (Pace, 2006); President George W. Bush signed Presidential Directive 54 that included the definition

“interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries” (White House, 2006); a "global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies” (Kuehl, 2009); “a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers” (Kissel, 2013).

Unlike the four physical domains, unique elements must be considered when employing situation awareness in cyberspace. First, the boundaries or geographic features are limitless. While the pilot may be able to view the world from the cockpit and even observe visually the elements of the environment, the elements for cyberspace consists of a digital representation, with information presented to the analyst through visual displays, intrusion detection alerts, and firewall or event logs. While the analyst may be able to understand the limit of the internal network, cyberspace is limitless. Second, the rate of change within cyberspace occurs at a much faster rate than the environment in the physical world. New attack methods, vulnerabilities, and exploits are continuously being designed and deployed along with new security technologies to counteract the attacks. Using air combat as an example, the rate of new attacks methods within the realm of cyberspace would equate to a new aircraft with the latest weapons appearing instantly

without warning. Based on the speed in which an attacker could penetrate a network would equate to compromising a friendly aircraft weapons system and deploying its armament without warning (Tyworth et al., 2012). Situation awareness incorporates the ability of the individual to use mental models that provides a mental representation of the environment. Changes are compared to the model to aid in determining whether a course of action should be taken. However, in cyberspace, changes occur at such a rapid pace that the use of mental models for the analyst is all but obsolete.

Cyber situation awareness is considered to be an extension of Endsley's model of situation awareness, but is applied to computer networks. However, in the context of cyber, situation awareness includes a mission awareness through the analysis of network events as it relates to the mission or goal being carried out by the organization (Doupé et al., 2011). While situation awareness can be achieved through the senses of the environment (touch, smell, sight, sound), cyber situation awareness is achieved through the gathering of data from various technological sensors, such as intrusions detection systems, firewalls, system monitoring software and related storage logs (Franke & Brynielsson, 2014).

Within the realm of cyberspace, situation awareness is perceived as a three phase process similar to Endsley model: situation perception, situation comprehension, and situation projection (Barford et al., 2010). The first phase, situation perception, is based on recognition and identification, which is the ability to identify the type of attack as opposed to only an understanding that an attack is in progress. Perception is more than obtaining data from intrusion detection systems. While usually a sensor on the network,

intrusion detection does not identify or recognize whether an attack is in progress, but simply identifies that an event, which may be part of an attack is in progress. Additionally, it is important to gain knowledge of the source of the attack and the intended target. To supplement this knowledge, the source or system of the information must be trustworthy or of high quality so as to gain confidence in recognizing an actual attack as opposed to a false alert. The second phase, situation comprehension, relates to impact assessment and adversary behavior. Being aware of the impact of the attack is acknowledgement of an attack in progress and assessing the damage in addition to an assessment of future damage as a result of the attacker continuing on the current path. To supplement the assessment of future damage is an awareness of the adversary's behavior based on attack trend and intent analysis. Additionally, the comprehension phase includes an awareness of why and how the situation occurred through back-tracking or forensics. In other words, focus is more on the behavior of the adversary than on the situation. The third phase, situation projection, is the ability to access possible future actions of the adversary as well as the path that may be pursued. To adequately project the future situation, an understanding of the adversary through intent, opportunity and capability as well as knowledge of the vulnerabilities within the environment is necessary.

The advancement in technology has presented organizations with security devices to detect threats launched against a network. However, these devices operate on known or predefined rules, such as a firewall, and experiences difficulties when confronted with unknown or undefined rules (Cummings, Bruni, & Mitchell, 2010). Vulnerability and threat information from network sensors alone are not adequate to provide the necessary

information in which to formulate an effective decision (Kornmaier & Jaouen, 2014). The decision-maker needs more than just to mitigate the existing threat, but the ability to counteract the cyber threat. Security devices will have difficulties in predicting future states of the environment as defined in level three of situation and cyber situation awareness. Security devices, both hardware and software exhibit proficiency in collecting, assimilating, and filtering relevant data for review but is primarily restricted to threats that are known and have been defined. The security analyst exhibits proficiency in areas that are lacking in today's technology to include the ability to interpret, analyze, and make decisions based on the information provided (Jones, Connors, & Endsley, 2011). However, with the amount of data presented for analysis by the security devices and the dynamic nature of the environment, the decision-maker is easily overwhelmed in attempting to gain the required level of cyber situation awareness. Attacks against organizational networks have increased through zero-day vulnerabilities, Botnets, and Distributed Denial of Service. Hacker tools are more sophisticated and have created an imbalance of capabilities between the attacker and the defender (Hernandez-Ardieta et al., 2013). The speed in which attacks occur are barely measurable as they occur at the speed of light (Clarke & Knake, 2010). Decision-makers who have achieved an acceptable level of situation awareness obtain relevant information through observing the environmental changes based on the current mental model, making sense of what the changes are, and if continuing on the current path, the implications in relation to the goal. Once the projection of the future state is determined, then a course of action is implemented. While this may benefit addressing changes in the physical domain, this

approach continues to be reactionary in the realm of cyberspace. Organizations continue to spend funds for new and more advanced security technologies, but the adversary continues to penetrate the defenses (Baker et al., 2012; Ponemon Institute, 2012; Verizon, 2013).

Cyber Intelligence

A growing recognition within the information security industry realizes the traditional security measures, including software and hardware, are no longer effective in counteracting the latest threats. The paradigm needs to change to include examining the security defenses from the viewpoint of the adversary. To address this change, the organization needs to implement an intelligence-based defense in conjunction with cyber situation awareness designed to improve the information security posture due to the rapid changes in cyberspace (Beer & von Solms Basie, 2013). The process of intelligence is essential as it supports obtaining an accurate awareness of the situation as well as an assessment of future developments based on threats, which is necessary in the decision-making process (Biermann, Hörling, & Snidaro, 2009; Kornmaier & Jaouen, 2014). In the cyber domain, intelligence may enhance the decision-maker's ability to detect the threat and perform an assessment of the cyber capabilities of the adversary. With the advance information through the intelligence process, the threat may be mitigated based on a proper evaluation of the effects of the attack resulting in improved security based on well-informed decisions (Gendron & Rudner, 2012). Intelligence increases the possibility to anticipate and mitigate future intrusions in the cyberspace environment based on the knowledge of the threat and is advantageous in studying the intrusions from the

perspective of the adversary (Hutchins et al., 2011). Intelligence for cybersecurity is not just the ability to understand network operations and activities, but also to understand who is performing the activity, why it is occurring, and what may be next phase of the activity. This includes collecting and analyzing data that is transformed into meaningful information that produces timely reports for the decision maker (Tamjidyamcholo, Bin Baba, Shuib, & Rohani, 2014; Hurley, 2012). Cybersecurity cannot rely solely on responding to known threats. The process must include tracking capabilities, intentions, and activities of the adversary, which is foundational to cyber intelligence. Specifically, the intelligence activities can discern who may be targeting the network; what are his or her capabilities and intentions; when will the malicious activity occur; where will the threat originate; how does he or she plan on penetrating the network (Mattern et al., 2014).

In a recent survey of approximately five thousand security professionals world-wide, forty-four percent stated that current security solutions do not provide adequately security intelligence to inform them of an attempted attack and the potential consequences. Fifty-three percent stated it is difficult to keep track of the security threat landscape (Ponemon Institute, 2014). One of the challenges of cyber intelligence is that no single organization has the relevant information regarding the threat landscape to maintain effective situational awareness (Barnum, 2012). Taking into consideration the overall threat landscape, the volume of data in relation to relevant threat intelligence, and the speed in which attacks occur, it is necessary for organizations to share this knowledge with each other. While trust between organizations sharing threat information is

necessary, this approach shares vital information as to what to look for so as to identify the attack and the attacker. The threat, or attack, that one organization battles one day may the next attack another organization battles another day. In sharing information as to what was observed and lessons learned from the attack, then others may be able to identify the attack in its early stage before an actual breach occurs on the network. It is also essential to share the information so that countermeasures effective for one organizational environment may be implemented in another organizational environment.

For the organization to protect themselves from known threats, an awareness and understanding of the latest threats is critical to the process. To gain this awareness, the flow of threat intelligence information is critical. Threat intelligence data may be gathered internally through the collection and analysis of network data, but more effective is obtaining intelligence through external sources such as cyber security companies. These external sources are valued by some organizations as the information and sources are validated and is considered as providing quality and relevant threat information (Haass, Ahn, & Grimmelmann, 2015). However, the issue still remains in how to effectively share the information, with whom should the information be shared, and what information will be relevant. Even with the available information and several forums and organizations participating in the sharing of threat intelligence, a significant number of organizations continue not to participate. According to a survey of 692 technology and security professionals, it was reported that forty-seven percent experienced a significant security breach that compromised the networks and data (Ponemon Institute, 2015). Over sixty percent of those experiencing the breach stated that

threat intelligence could have prevented the attack or minimized the consequences of the attack. While threat intelligence may be essential to support a strong security posture for the organization, the same research study showed forty percent did not participate because of a lack of trust in the source of the intelligence, the process of sharing was too slow, and the perception of sharing of threat intelligence was not beneficial to the organization.

Summary

The ability of the security professional to maintain situation awareness and adequately defend the security posture has been reduced due to the complexity of the global computing environment coupled with the speed in which information transverses the Internet. Even with enhancements of security technical devices and advanced software, the defense methods remain in a reactive mode. Research has shown that utilizing current security methodologies and relying on technology alone does not adequately support the requirements to meet the current challenge of attacks. Organizations have begun to examine the benefits of implementing threat intelligence to enhance the organization's information security program. Understanding the value of implementing threat intelligence may encourage more security professionals and organizations to modify the current methodology and create a paradigm shift from reactive to proactive protection.

Chapter 3 explains the research methodology to be conducted for this study. It provides an overview of the qualitative approach, data collection and the analysis, participant selection and procedures.

Chapter 3: Research Method

Introduction

I utilized a qualitative methodology with a case study design. The goal was to gain an understanding of the impact of incorporating threat intelligence into the cyber situation awareness model for the decision making process as it related to an attack against an organization's security posture. In addition, the study was to help understand if advanced indicators of an attack were present in network monitoring devices (firewalls, routers, antivirus, etc.) and whether utilizing the concepts of cyber situational awareness could have prevented a successful attack. The research method was reviewed by Walden University's Institution Review Board and granted approval for the research. The approval number for this study was 07-21-16-0064526.

Information security is in need of a change from reactive to proactive defense and must include the ability to understand the motives of the attacker as well as the tools and methods used in attacks. Knowing in advance what unusual patterns provide evidence of an attack, determine the specific system and/or process against which the attack is directed, or the types of information that are the target of the attack will improve the organization's ability to proactively increase security measures where necessary. Intelligence through the sharing of information between organizations provides the advantage of shifting from reacting to an ongoing attack to becoming proactive in understanding the threat, intent, and motives of the attacker and reduce the likelihood of a successful attack (Hutchins et al., 2011).

Little research has been provided that identified the value of available shared information through threat intelligence that is necessary for the security professional or decision-maker to make a qualified decision (Tadda, 2008). The purpose of this study was to explore whether the value of current threat intelligence may increase the security analyst and decision maker's situation awareness so as to detect a potential adversary's intention.

Based on the methodology of case study research, the questions this study was designed to answer were:

RQ1: How effective is situation awareness in response to cyber-attacks?

RQ2: How does threat intelligence support situation awareness in response to cyber-attacks?

RQ3: How difficult is maintaining situation awareness for information security?

RQ4: What effect on information security was due to the combination of threat intelligence and situation awareness?

RQ5: Why was implementing threat intelligence with situation awareness successful or unsuccessful in the goal of information security?

In the major sections of this chapter I address the research design and rationale in approaching the study. I compare the various design methodologies along with the reasons for not selecting a specific design. I also provide the reasons for the selection of a case study and the rationale as to why this approach was best for this study. For this study, my role as researcher included conducting interviews, making observations, and

reviewing available supporting documentation. The methodology I used was to interview information security professionals to understand the process involved in deciding whether incorporating cybersecurity intelligence added value to the decision making process. A pilot study was conducted with the purpose of validating the questionnaire and determining whether any questions were misleading or required additional clarification.

Research Design and Rationale

The study purpose was to understand the value in integrating cyber intelligence into the process of situation awareness for information security professionals who are responsible for protecting an organization from and reacting to cyber threats.

The purpose of qualitative research is to gain an understanding of issues or a particular situation by investigating the perspectives and behavior of the individuals involved in these situations and to study the context in which they act (Kaplan & Maxwell, 2005, p. 30). This means understanding the meaning of the events, situations, experiences, and actions from the perspective of the participants (Maxwell, 2005, p. 22). Qualitative research methods are useful for evaluating experiences and the decision process that is not adequately captured through quantitative methods. Qualitative methodology was best suited for this study as it allowed me to examine the proposed problem statement as actually experienced by the individual as opposed to "second hand" experience (Patton, 2002, p. 104). Most qualitative research is based on an interpretivist perspective. Interpretivism holds the perspective that truth is contextual, depending on the specific situation, the individuals who are being observed, and the researcher performing the observation (Chism, Douglas, & Hilson, 2008, p. 2). This approach

supported the study as each cyber threat characteristic was different, occurred under different circumstances, and was approached through different methods by the security professionals.

Various methodologies of qualitative research were examined to determine the best approach for this study. A narrative study was considered as it allowed the research to describe stories through the study of one or more individual's experience, using interviews and looking for themes in the data. However, a narrative study was not appropriate as it examines an individual or group of individuals' life with the final product being a chronological narrative about the participants experiences. Grounded theory examines multiple individuals who participated in a process and generates a theory grounded in the data collected. While grounded theory is consistent with some of the research, it did not address adequately the purpose of the research as this study was not to generate a theory but to examine integrating cyber intelligence into the security program. Ethnography examines groups that share a culture and focuses on describing or interpreting that shared culture. The purpose of this study was to examine a specific issue rather than a sociocultural attribute; therefore, this approach was not appropriate (Creswell, 2007). Phenomenological researchers collect data through use of interviews, observations, and existing documents, which was consistent with the data collection approach of this study. The data analysis strategy was also consistent with this study as the researcher looks for significant statements, meaning, and textural descriptions to draw conclusions. Phenomenology was not appropriate, however, as the focus was not to understand and describe a lived experience.

Case based research was the best choice for examining the incorporation of cyber intelligence processes with situation awareness within the organizational security posture and therefore was the most appropriate methodological design for reaching the goal of this study.

A case study is preferred when the focus of the research is to answer *how* or *why* questions, examining events that are contemporary and where relevant behaviors cannot be manipulated and the contextual conditions are relevant to the phenomenon being studied (Baxter & Jack, 2008; Yin, 2009). It also incorporates direct observations and interviews of the individuals who are actually involved in the events that are being studied (Yin, 2009, p. 11). It is useful in understanding the casual chain that results in either success or failure by revealing in chronological manner the actors and events that influenced the final outcome (Benbasat, Goldstein, & Mead, 1987, p. 382). A multicase approach was appropriate for this study as it focused on more than one specific case in depth that provided an in-depth understanding. Multicase studies examine multiple sources of data collection including interviews and observations and provide a detailed analysis of each case and an overall conclusion found among all cases.

Role of the Researcher

I have 30 years' experience in the field of information technology and over 20 years' experience specializing in the area of information security. I am certified through SANs Global Information Assurance in Security Audit and Control and a member of InfraGard, a collaborative group consisting of agents of the Federal Bureau of Investigation and local organizations. The main purpose of this study was to share

information relating to the latest threats in cyberspace. My current role is manager of information security (governance, risk and compliance) for a large healthcare organization located in the metropolitan area of St. Louis, Missouri.

For this study, my role as researcher included interviews, observations, and reviews of available supporting documentation. Since the study was performed within my organization or circle of influence, no relationship, whether personal or professional, was involved during the research. This study was performed with some bias based on my current experience with cybersecurity and participation in cyber intelligence information sharing groups. My bias is an assumption that cyber intelligence through information sharing adds value to the process of cyber situation awareness for an organization's information security program.

Methodology

Participant Selection Logic

The sample size in this qualitative research was based on the subject of the study, the purpose of the study being conducted, what information was useful, and the amount of effort available based on time and resources (Patton, 2002). Accordingly, no specific rules for determining the sample size in qualitative research was available. It was not possible for me to include every individual regardless of geographic location in the course of the study. The choices that were made about who to include and why places limits on sampling in the inquiry (Miles & Huberman, 1994).

In determining the sample size, purposeful sampling was used in this qualitative research study. Purposeful sampling is where the researcher selects individuals and sites

to study because they can purposefully provide in-depth understanding of the central problem. If the size is too large, the researcher may become overwhelmed with the volume of information, which may have an adverse effect on the study due to limitations of time and resources. Various researchers have suggested guidelines for determining appropriate qualitative sample sizes for case studies.(Charmaz, 2014) suggested that 25 participants are appropriate for small projects. (Ritchie, Lewis, Nicholls, & Ormston, 2013) stated that the sample size is often 50. (Green & Thorogood, 2013) stated that very little new information is derived after approximately 20 individuals are interviewed.

For the case study approach, 13 individuals were interviewed for the study. For this study I intended to interview information security professionals to understand the process involved in deciding whether incorporating cybersecurity intelligence added value to the decision making process. The individuals interviewed presented the opportunity to gain more in-depth, relevant data within the constraints of the study.

The criterion on which participant selection was based was through the use of established qualifying benchmarks. Individuals were to have a minimum of 5 years of direct information security experience. In addition, individuals were to have direct technical experience with network defense to include firewalls, routers, intrusion detection, and security event analysis. During the selection process, information gathered included employment history, security certifications, years of direct experience, specialized security training, and affiliation with any cybersecurity information sharing groups. While the participant population was 13 individuals, the objective of the research was to achieve saturation. Saturation occurs when no new information was added in order

to gain better understanding or the information becomes redundant (Patton, 2002, p. 246). Saturation, where no new information was obtained, occurred after the 9th interview.

Instrumentation

The basis for the instrumentation development was from literature reviews, my professional experiences within the information security field, and through a pilot study. The instrumentation was individual interviews through the use of a voice recorder. Interviews were used as a method to understand the cognitive and behavioral aspects of the security professional in decision-making process during and after a security incident. The interview session was guided through formal questions in order to maintain focus on the topic by both the interviewer and interviewee. The nature of the questions were to ascertain demographic data, qualifying data for the purpose of the study, and open ended questions pertaining to the nature of the study. The open ended questions allowed the interviewee to provide relevant information as well as professional opinions.

Pilot Study

A pilot study was conducted with the purpose of validating the questionnaire and to determine whether any questions may be misleading or require additional clarification. The study was to consist of four or five individuals being interviewed for approximately one hour. These individuals were selected based on the established criteria, but was not included in the formal study. Recruitment was selected from the study population and included participation based on the snowball approach where individuals recommended other qualified persons that may add value to the study. Each individual was provided

with the nature of the study and given the opportunity to either participate or to decline. A consent form was provided.

Procedures for Recruitment, Participation, and Data Collection

The target population for the study was professional security personnel who are actively involved in the information security for the organization. Participants may be performing the role of manager, security analyst, security architect, security administrator, or any other function providing his or her individual role or daily function was actively related in providing security for the organization. The participants were identified as fulfilling a variety of different security positions where other organizations may employ one professional for each role. Identification of specific organizations and individuals was not used in the study. Training in and technical experience and knowledge of information security was a primary criteria for the research study. Additional questions included in the survey were for use and data collection. The study population was to consist of companies primarily within in the St. Louis, Missouri metropolitan area.

The data was collected through interviews either by phone or in person. Individuals were contacted through electronic mail and invited to participate in the study. All perspective participants were informed of the nature of the study and the confidentiality of the information provided.

Data Analysis Plan

Pre-coding structure for qualitative data analysis refers to the creation of a provisional start list containing codes before conducting the fieldwork (Miles &

Huberman, 1994). Based on the list of research questions, key variables, and problems studied, the list of codes were developed. An advantage to creating codes prior to the start of fieldwork was that it forced the researcher to connect the questions or interests to the data (Miles & Huberman, 1994). In addition, using codes aided in identifying what was important among the vast amount of information gathered through various mediums (interviews, documents, records, etc.). Through the use of codes, the information was more organized and structured and reduced the time to analyze the data.

Issues of Trustworthiness

Credibility

Verification through the participant's feedback to what is described and the resulting conclusions provided the researcher confidence in the accuracy, completeness, and fairness towards the validity of the data analysis (Maxwell, 2005, p. 111; Patton, 2002, p. 560). Each participant upon completion of interviews was provided the opportunity to review the content and address and questions or concerns. For specific questions, an expert review provided an increase in the level of credibility through judging the quality of the data collection and analysis (Patton, 2002, p. 562). Through the review the researcher was able to verify whether the results were accurate in the interpretation of the information provided by the participants.

Transferability

Transferability is understanding whether the conclusions of the research study be applied to other studies or theories. To support transferability, the data, or information collected was sufficiently detailed and varied to fully understand the topic and the

process. Collecting the detailed information made it difficult to concentrate only on the data that supports any prejudices and preconceived expectations and was a test on any generating theories derived from the research study (Kaplan & Maxwell, 2005). In this manner, the researcher had the opportunity to discover new questions that may lead to new discoveries or actions.

Dependability

Dependability is whether the process involved in the research study is consistent and reasonably stable over time and across different researchers and methods. It addresses whether the research questions are clear and the data collected across appropriate times, settings, and participants as indicated by the research questions (Miles & Huberman, 1994, p. 278). Dependability was achieved through the concept of triangulation. Triangulation was the use of multiple and different sources or methods to corroborate the evidence gained by the researcher. This method reduced the risk that the conclusions of the study reflected only biases or limitations of a specific source while providing the researcher with a more broad understanding of the study by the researcher (Maxwell, 2005, p. 93). Dependability was based on quality and appropriate checks were implemented to provide assurance that appropriate care was undertaken during the research process.

Confirmability

Reflexivity is being aware of the researcher's contribution of the interpretation in the research process based on cultural, social, class, and personal positions (Cresswell, p179). I was able to determine that the conclusion of the research was dependent on the

inquiry and was not influenced by personal assumptions, values, or biases. I was aware and explicit about how these could have influenced the study (Miles, p 278).

Ethical Procedures

The nature of this study required gathering information that many security professionals consider confidential as it may outline specific security measures and procedures for the organization. It was imperative that the participants were given assurances that the information provided would be kept confidential and that the participants providing the information would remain anonymous as well as the specific organization. To address this specific point, the signing of a Non-Disclosure Statement was offered by each participant deemed to be unnecessary. All questions, processes, and survey instruments were disclosed to the Institutional Review Board for review and approval prior to the commencement of any fieldwork for this research.

All information and data collected was maintained in a confidential manner. The researcher did not use any information provided for any purposes outside the scope of this research study. All participants were required to sign a voluntary consent form approved by Walden‘s Institutional Review Board process. All documentation are kept locked and in secure storage device for future research request. Participants were informed that they have the right to stop providing information during the process without any risk or consequence.

Summary

The information in this chapter provided detailed information in conducting the case study as to the role of cyber intelligence within the process of situation awareness.

The data collected was through the use of survey questions and interviews with participants who meet the criteria established within the information security field. The data collected is kept confidential and used only for the purposes of this research study.

Chapter 4: Results

The purpose of this study was to examine the perceived value of threat intelligence information sharing as a proactive process for information security. The objective of this study was to explore how situation awareness is enhanced by receiving advanced intelligence reports resulting in better decision-making for proper response to security threats. In this chapter I present the results and findings of the qualitative research methodology following a case study approach. In this chapter I describe the process used to identify the participants, validate the instrument, gather the data through interviews, and analyze the data as related to each research question.

Based on the methodology of case study research, the interviews for this study were designed to answer the following questions:

RQ1: How effective is situation awareness in response to cyber-attacks?

RQ2: How does threat intelligence support situation awareness in response to cyber-attacks?

RQ3: How difficult is maintaining situation awareness for information security?

RQ4: What effect on information security was due to the combination of threat intelligence and situation awareness?

RQ5: Why was implementing threat intelligence with situation awareness successful or unsuccessful in the goal of information security?

Nvivo software was used to analyze the responses to the interview questions. A summary of the results is presented at the end of this chapter.

Pilot Study

The pilot study interview consisted of conducting one hour sessions with three individuals. The selection procedure consisted of selecting qualified pilot participants obtained from public information contained on LinkedIn networking website.

A pilot study was conducted to validate the questions for the interviews as to their clarity, purpose and relevance to the research questions. The research questions were designed to explore the concepts of the study. Additional questions have been identified and can be defined as issue questions. These questions are not informational questions but provide the opportunity to prompt the participant to a deeper level of critical reflection of the core process of the study (Stake, 2013). Initially, 25 issue questions were designed to explore to a deeper level of each stated research question. Through the use of the pilot study, each issue question was reviewed for the intended meaning and objective to avoid any misleading or inadequate responses and to determine if the content of the questions was too intensive for comprehension. The pilot study added value as it provided the opportunity to make improvements and adjustments to the main study (Kim, 2011).

The interview for each participant lasted 45 minutes to 1 hour and each question was discussed to determine its overall value to the study. The result of the pilot interviews provided the opportunity to reduce the number of issue questions from 25 to 14 in order to avoid duplication. The actual research questions were reviewed and determined that original RQ4 and RQ5 were closely related and should be rewritten to be combined as one question. Another determination was defining the term “situation

awareness" for the participants. This term has different meanings based on the participants' perceptions and may not be consistent with the definition of the study. In other instances, while the concepts of situation awareness is used in daily activities, participants may not be aware of the actual term.

Research Question	Supporting Interview Questions
Question 1: How effective is situation awareness in response to cyber-attacks?	Describe how you were alerted to this incident? How much time did it take to remediate the incident? Describe any additional investigations performed related to the incident after remediation? What factors were included in your decision making to respond to this incident?
Question 2: How does threat intelligence support situation awareness in response to cyber-attacks?	What sources do you rely on to keep abreast of the latest security threats? Are you a member of any cybersecurity information sharing groups? If not, why? How effective is your participation with cyber intelligence information sharing in your organization's information security program? How accurate is the information you receive relating to the latest threats?
Question 3: How difficult is maintaining situation awareness for information security?	With several servers generating various event logs and a high number of alerts, how do you monitor them to identify any real or significant incidents? Do you believe the analyst is able to do an adequate job in analyzing and determining what events are going on? How effective do you believe situation awareness is in responding to cyber-attacks?
Question 4: How effective is threat intelligence in support of information security?	Describe the reasons for participating in cyber information sharing groups. Do you believe that threat intelligence could have minimized or prevented the consequences of your incident? Why or why not? Describe the main elements of a cyber intelligence information sharing program that would be (or is) most important to you.

Figure 3: Matrix of research and issue questions.

Research Setting

The setting for the research interviews were varied based on the participant and the participant's geographic location. Two interviews were conducted in the individuals' business locations in the St. Louis, Missouri, metropolitan area. Three interviews were performed in a private office and one in a secluded conference room. The remainder of the interviews were conducted as phone interviews due to either available time or geographic location. The target geographic location centered towards the St. Louis, Missouri, metropolitan area; however, the qualifying criteria did not restrict the participants based on geographic location. Phone interviews were conducted with one individual in Washington, DC, one individual in Kansas City, Missouri, one individual in Jefferson City, Missouri, one individual in Baton Rouge, Louisiana, and seven individuals in St. Louis, Missouri. Each participant established the date, time, and, where appropriate, the location for the interview.

The interviews lasted 45 minutes to 1 hour and were recorded using a digital audio recorder. The initial conversation, which lasted 5 to 10 minutes and included a personal introduction and brief description of the study, was not recorded.

Demographics

Participants selected for this study were determined based on specific criteria or purposeful sampling method. With purposeful sampling, the researcher seeks to gather as much information as possible in order to understand the important issue of the study from the participants' perspective. It is vital to select participants from whom the most information may be obtained (Merriam, 2002).

Specific personal information was not asked of the participants. Demographic information such as age and gender were discovered through viewing public professional profiles as listed on the website LinkedIn but was not relevant to the requirements of the study. LinkedIn is a free public site for individuals and companies to publish professional profiles and contact information with the purpose of collaborating with peers on related professional topics or as a recruiting tool for companies searching to locate individuals for hire. In addition to using LinkedIn, I contacted individuals for participation through previous professional relationships and those whose qualifications were well known. The criteria for participation consisted of (a) a minimum of 5 years' experience in the information security field; (b) a current role within the organization in or directly related to information security; and (c) background including direct experience with network defense to include firewalls, routers, intrusion detection systems, and security event analysis. Seniority level was not a main consideration or requirement for participation but included CEOs, CIOs, senior directors, managers, and security analysts. The CEOs met the criteria as they currently led companies in the information security field and had technical backgrounds. The other participants represented various industries to include government, financial, health care, and professional services. The selection of participants were purposeful in order to gain an understanding of the level and type of information necessary at each level of the organization so that informed decisions may be made. In the sample population, 85% were male, 23% were junior level positions, 46% were mid-level, and 31% were senior level positions. The experience in the security field ranged from 10 years to 30 years with the average experience of 17 years. The following

figure provides the specific qualification of the participants for this study and whether the participants personally participated in a cyber intelligence program.

Participant Code	Position	Geographic Location	Years of Technical Experience	Industry	Cyber Intelligence Participation
Participant 1	Manager	St. Louis, MO	14	Financial	No
Participant 2	CEO	St. Louis, MO	18	Technical Services	Yes
Participant 3	CEO	Washington, DC	18	Government	Yes
Participant 4	CIO	St. Louis, MO	30	Financial	Yes
Participant 5	Director	St. Louis, MO	14	Technical Services	Yes
Participant 6	Director	St. Louis, MO	12	Managed Services	Yes
Participant 7	Security Architect	Peoria, IL	22	Healthcare	No
Participant 8	Director	St. Louis, MO	20	Government	No
Participant 9	CEO	St. Louis, MO	24	Technical Services	Yes
Participant 10	Director	Kansas City, MO	20	Healthcare	No
Participant 11	Director	Baton Rouge, LA	10	Healthcare	No
Participant 12	Security Analyst	St. Louis, MO	10	Healthcare	Yes
Participant 13	Security Analyst	St. Louis, MO	10	Healthcare	Yes

Figure 4: Participant demographics.

Data Collection

The data collection process was conducted over a seven month period screening for potential participants, conducting a pilot study, and initiating participant interviews.

Potential participants' professional profile was screened through the free public LinkedIn web site. Professional group members were screened and 850 were identified with the qualification criteria outlined for this study. Invitations were sent to these potential participants and 165 requested additional information about the study and 13 agreed to participate. Originally, the projected number of participants was estimated at 30. The outcome of the study was not adversely affected with the lower number of actual participants. No new information relating to security processes or threat intelligence was gained after 9 interviews resulting in the achievement of saturation. The data was collected through personal one-on-one interviews with 13 individuals. Two interviews were conducted face-to-face in an office environment of the participant. The remaining interviews were conducted as phone conferences due to geographic locations and available time. The interviews were guided through the set of questions resulting from the pilot study and designed to facilitate the conversation, but allowed the participant to expand on the topic as needed. Each interview was recorded on an Olympus digital voice recorder, model WS-853. The recorder timestamps each interview with the time/date and unique identifying code in an MP-3 format. In addition, each interview was stored in a separate folder on the recorder. During interview, I took handwritten notes in addition to the recording in the event any additional clarification may be necessary during the conversation.

A change was made in the data collection process as described in Chapter 3. Originally, an on-line survey instrument was identified to gather the data for the study. While the survey would provide some information, an interview process was decided as

the best approach as it offered the opportunity for the participants to expand on the questions in more detail.

Data Analysis

Analysis of the data collected began with the transcription of the interviews from digital recordings to text documents using Microsoft Word 2013. The transcriptions' accuracy was verified by reading the text while listening to the audio recording. The documents were provided to each participant for review and verification of the information. The text of the interviews were imported into the analysis software NVivo Starter Edition version 11. The analysis provided a listing of the most common words used by the participants for each of the research questions. The criteria for the frequency pattern was the word of at least 8 characters in length, matching the word and stems, and generate a list of the 50 most frequent works. Displaying the list in a Word Cloud format, I was able to generate various nodes to further analyze the data and the context of word usage. By comparing the data across the nodes I was able to identify significant themes and correlate the themes with each research question.

Research Question	Theme
Question 1: How effective is situation awareness in response to cyber-attacks?	Process for threat reporting Analyst training
Question 2: How does threat intelligence support situation awareness in response to cyber-attacks?	Proactive security Risk Identification
Question 3: How difficult is maintaining situation awareness for information security?	Volume of data Speed of breach
Question 4: How effective is threat intelligence in support of information security?	Quality of threat intelligence Source of threat intelligence

Figure 5. Themes.

Evidence of Trustworthiness

Credibility

Verification through the participant's feedback to what was described and the resulting conclusions provided confidence in the accuracy, completeness, and fairness towards the validity of the data analysis (Maxwell, 2005, p. 111; Patton, 2002, p. 560). Each participant upon completion of the interview was provided the opportunity to review the content and address any questions or concerns. In addition, the use of an expert review provided an increase in the level of credibility through judging the quality of the data collection and analysis (Patton, 2002, p. 562). I solicited the opinion of several professionals with in-depth experience in the areas of firewall administration, computer forensics, cyber security, network security administration, and information security event analysis. These individuals expressed confidence in the approach of the research and provided a validation of the research theory.

Transferability

Transferability is understanding whether the conclusions of the research study be applied to other studies or theories. The data collected through the participant interviews and analysis of the data through analytical software is sufficiently detailed to fully understand the topic and the process. In collecting the detailed information of cyber intelligence as it supports situation awareness, I was able to concentrate not only on the data that supported my expectations but through the interview process had the opportunity to discover new questions to link the results to other studies or theories.

Dependability

Dependability was achieved as the process involved in this research study would be consistent and reasonably stable over time and across different researchers and methods. The research questions were clear and the data collected across appropriate times, settings, and participants as indicated by the research questions would achieve the same results (Miles & Huberman, 1994, p. 278). Dependability was achieved through the concept of triangulation. Triangulation is the use of multiple and different sources or methods to corroborate the evidence gained by the researcher. This method reduced the risk that the conclusions of the study reflected only biases or limitations of a specific source while providing the researcher with a more broad understanding of the study by the researcher (Maxwell, 2005, p. 93). Dependability was based on quality and that appropriate checks are implemented to provide assurance that appropriate care was undertaken during the research process.

Confirmability

Reflexivity is being aware of the researcher's contribution of the interpretation in the research process based on cultural, social, class, and personal positions (Cresswell, p179). The researcher needs to determine whether the conclusion of the research depends on the inquiry or is influenced by personal assumptions, values, or biases. The researcher needs to be aware and explicit about how these may have influenced the study (Miles, p 278).

The research conducted for this study drew its conclusions from the inquiries of the participants and was based on individual professional experiences. I have several years of experiences within the information security field, but I did not inject any personal assumptions or biases that would influence the conclusion of this study.

Study Results

This qualitative research study was a case study approach to understand through the experiences of the participants as to how cyber intelligence provides support to situation awareness for information security. Each interview began with an overview of the purpose of the study and the format for the interview process. Each participant was informed that while specific questions would be asked during the interview, these questions were designed to facilitate the interview and each participant was encouraged to provide as much detail as they desired to communicate. Each participant was also informed that the study did not require the participant to reveal any proprietary or confidential organizational information. Each interview lasted between 30 minutes and one hour, with the average interview lasting 45 minutes.

Each participant was familiar to a certain degree the meaning of situation awareness. The most common perception of the meaning was the awareness of events occurring at any particular moment in time. Awareness is a portion of the definition of situation awareness and to be consistent, the three parts of situation awareness was explained and the relation to this study. It was not necessary to know of any specific cyber-attack or the technical details. To understand the effectiveness, it was important to know the process of alerting about the incident, how much time was involved from alert to action, and what factors were included in the decision-making process in responding to the incident.

Research Question 1

RQ1: How effective is situation awareness in response to cyber-attacks?

The cyber environment in which organizations participate and operate rely on the security devices deployed to protect itself from unauthorized activities. For the future, the ultimate goal is to devise a security foundation based on artificial intelligence that will provide protection without the intervention of human decision-makers. While this goal is one that may be realized in the future, this role is performed by the security analyst who is responsible for observing the operations within cyberspace, understanding any changes and its consequences, and determining the proper response (Dutt, Ahn, & Gonzalez, 2011). The research question strived to examine the effectiveness of the analyst's ability to understand the changes and determine the appropriate response to a cyber-attack based in his or her cognitive situation awareness within the cyber environment.

Security devices designed to monitor network activity will provide alerts when an event violates a rule, but security analysts also receives alerts from a variety of sources. Participant 11 stated different scenarios contribute to situation awareness. The information could come from the operations center, the security analyst's observation, or receiving alerts from the security devices that a potential breach or attack is in progress. In learning how the alert process occurs, Participant 9 stated that awareness is not always from an observed state, such as logs relating to system events or firewall alerts. Awareness may generate from an end user, who in turn may notify the administrator that an anomaly has been observed. These sources generate a large volume of information that may be valuable but overwhelms the analyst. Sometimes, according to Participant 9, the information turns out to be old or benign and not usable for decision-making. Regardless of the source of the alert that comes to the security analyst, the analyst uses the mental process of fusing the various pieces of information together and comparing this to the analyst's mental picture of the current network. Participant 12 stated that based on the current mental model of the network, when it is noticed that something appears that may be an anomoly, it stands out and grabs the attention of the analyst.

Timing from notification to action is an important factor in determining the effectiveness of situation awareness. According to Participant 5, "the timing of notification can vary depending on the pathway that the attacker is taking." Participants have stated that notification of an actual attack is dependent on different factors, such as if it is a firewall alarm, slow periodic events that trips a specific rule, and the type of

systems that are being hit. Depending on the pathway, this could result in minutes to hours before notification of the attack.

Once notified of an event, another factor in situation awareness is projecting the consequences of the event based on the criticality of the system or systems being attacked then implement an appropriate response. According to Participant 8, a variety of factors are involved that are running through the analyst's mind that he immediately wades through the mental processes as to the appropriate response. Participant 7 supported this view and stated that if it is critical, then "you act on it immediately. The minute you hear about it, you isolate the system, kill the account so it no longer has privileges on the network." Participant 5 agreed that the decision is based on the criticality of the system: "it's an instantaneous decision. We shut it down, period, end of statement." Other factors considered in the decision-making process include whether the system contained non-critical data or data that is not significant; do the event logs provide any insight into the activities; is it virus, malware, or an actual penetration attempted by an unauthorized individual or group.

The speed in which attacks can occur can be measured at the speed of light and be considered as zero-day exploits (Tyworth et al., 2012). The speed in which new attack methods are being developed and deployed and new vulnerabilities discovered and exploited, it is very difficult for the security analyst to solely rely on his situation awareness and security devices to counteract these events.

The data in this study revealed that relying on the analyst's situation awareness to identify cyber-attacks that are occurring within the network and to understand the

consequences against the security contributed to the overall security defenses but did not provide enough intelligence on its own to support an effective security defense. Participant 2 stated that in most instances when the analyst discovers the event it is "almost too late to make a good decision to respond or not." The security analyst contends with a large volume of potential cyber-attacks that are reported through logs and alerts generating an overload of information. It is difficult for the security analyst to rely on only one source of intelligence, namely his or her situation awareness ability, to comprehend the changes that are occurring and project the consequences so as to make well-informed decisions for a proper response.

Research Question 2

RQ2: How does threat intelligence support situation awareness in response to cyber-attacks?

Relying on the analyst's situation awareness to identify and comprehend the events that are occurring within the network provided an inward view of how the attacker is penetrating or attempting to penetrate the security defenses. This view of the event and related information does not provide effective security advice for decision-makers and is mainly a technical point solution. (Kornmaier et al., 2014). Participant 1 stated that while situation awareness is effective, it's going to be reactive "because we're looking at logs and the logs are going to tell us past events." Information that is necessary for the decision-maker is provided through the intelligence process and increases the accuracy of situation awareness through anticipating intrusions based on the knowledge of the threat

(Hutchins et al., 2011). The research question strived to explore how utilizing threat intelligence supported situation awareness in defending against cyber-attacks.

The data in this study revealed that threat intelligence is able to point the security analyst towards specific point of entry or exploit of a specific vulnerability as well as indicate a specific type of attack that may be targeting an industry or organization. The participants agreed that utilizing threat intelligence is a valuable process that strengthens the organization's security procedures as it narrows the focus of the analyst towards the potential threat. Participant 7 stated that the intelligence information received shows what vulnerabilities a particular threat is exploiting and provides the security analyst the advance knowledge to strengthen any necessary security defenses. Participant 10 agreed with this viewpoint in that threat intelligence is able to provide an awareness of events that may not be noticed under normal monitoring conditions. The advanced information provides the avenue to examine various configurations, identify any risks based on the intelligence received, and in turn, be aware of any changes outside of normal processing that may lead to identifying a potential breach.

Threat intelligence provided additional support to the security analyst by providing insight into the consequences of the potential attack as well as the possible motivation of the attacker. Participant 3 stated that while the first victim may not be successful in stopping the attack or minimizing the consequences, sharing the intelligence can greatly benefit the other organizations so as to either minimize the damage or even prevent the attack. This information is more than identifying bad IP addresses or hash files known to be suspicious in nature. Effective support for situation awareness is where

the security analyst is presented with details of underground chatter in the darknet, gathered through human intelligence alerting the organization of the probability of an attack, the method deployed, and the specific information to be targeted in the attack. Supporting this view, participant 9 related that it is important to gather all the pieces of intelligence data and fuse this information together so that the security analyst gains full situation awareness across the enterprise. In fusing both the technical and the human intelligence and applying the information to the mental process of understanding the threat, the analyst may be better prepared to form a decision for response.

Research Question 3

RQ3: How difficult is maintaining situation awareness for information security?

Situation awareness represents a security analyst's ability to interpret events within the observed environment. The security analyst must remain aware of the state of the environment and be able to anticipate critical situations as they emerge so as to understand the consequences and take appropriate action. However, the analyst's ability to maintain an accurate level of situation awareness is severely affected through information overload, time criticality as well as the speed of the events as they unfold. The results can be a partial loss of situation awareness or a complete misinterpretation of current situation (Salfinger et al., 2013). The research question strived to examine specific variables that contribute to the difficulties in maintaining situation awareness.

The security analyst is presented with the task of identifying anomalies that occur within the network, understanding what these events mean to the security of network and project the consequences. Due to the speed of data processing and the vast number of

servers within an organization, the analyst is constantly in a reactive mode. Participant 8 believed the difficulty is in the many variables. Does an accurate baseline exist so the analyst can determine if it is normal traffic? Is the proper technology in place, such as a SIEM or something reporting information to increase the analyst's situation awareness? Participant 4 stated that the difficulty also resides knowing what else was going on within the system. "The bad guys are getting pretty smart and they will DDoS you on the front end and then try to come in the back." Other variables that make maintaining situation awareness is the low and slow attacks. These attacks stay under the threshold of generating alerts by the security devices and can take a significant amount of time to identify the patterns. Participant 2 stated that it is difficult for human beings to be able to put all the information together that might be available to give an indicator of the risk and changes in behavior. Participant 11 stated that much of the information generated through alerts is repetitive and trying to correlate with the various systems looking for similar patterns is time consuming and a challenge for any analyst to maintain adequate situation awareness.

The volume of data and the speed in which the data processes are main factors that contribute to the difficulty in maintaining situation awareness. Situation awareness is based on the cognitive ability of the security analyst to construct a mental picture of the network or infrastructure so when changes occur the analyst is able to determine the significance. As new vulnerabilities are discovered and new or updated security devices and/or applications are implemented, the security analyst must update his mental model of the infrastructure so a current mental diagram is maintained. Because of the speed and

frequency of changes, it is extremely difficult for the security analyst to maintain a current mental diagram so when a potential or active cyber-attack occurs, the analyst is comparing the consequences to an outdated mental model. This diminishes the ability of the security analyst to maintain his situation awareness to effectively support the organization's information security program and security goals.

Three of the participant's offered another variable attributing to the difficulties in situation awareness. The analyst needs to be knowledgeable to be able to identify and react properly to the potential threat. Organizations are deploying various devices to alert the security staff of any potential threat or risk to the data. One issue is the analyst continues to monitor these devices and relies on these devices inform them of any intrusion into the network. The alerts generally are illustrated through a color scheme indicating informational, caution, or critical. Waiting to interpret these indicators can be misleading as it is dependent on what it knows and what has been seen in the past. Participant 9 stated that the attackers have the same technology and they are writing malware "so it can't be seen, or it doesn't bubble up to a red or flashing alert". Organizations have advanced systems that are properly configured and issuing alerts, but as Participant 8 added "if you don't have the staff knowledgeable enough to deal with it, then you don't have adequate situation awareness". To compliment situation awareness, the analyst needs a deeper training beyond what the application or security device teaches or the vendor teaches about the application. Participant 10 added that additional training will enable the analyst to look at the events and make proper decisions, and "helping them to have proper situation awareness."

Research Question 4

RQ4: How effective is threat intelligence in support of information security?

Organizations rely on the traditional security measures contained in both hardware and software solutions even though these solutions provided minimal protection against cyber-attacks. The collection of logs and the analysis of events as reported by these solutions do provide a certain level of security that is valuable, but due to globalization and the complexity of cyber security generates a difficult landscape for the security analyst. A consensus has emerged that it is necessary to share information about threats, actors, tactics, and motivations in order to develop and maintain an effective cyber security defense (Hernandez-Ardieta et al., 2013)(Hernandez-Ardieta et al., 2013). The research question strived to examine the effectiveness of threat intelligence in support of an effective cyber security program.

The majority of the participants expressed the view that threat intelligence is an effective mechanism in supporting information security. The intelligence that is received has been especially effective in that it provides insight into threats and vulnerabilities that may be considered zero-day events, targeted attacks due to political events, social exploits based on tragedies or religious events or new malicious software to further criminal activities. This information has changed the security process from a traditional reactive mode to a proactive mode and allowed the decision-maker to understand the risks and level of criticality in order to make a better informed decision as to the proper course of action. Participant 2 stated that threat intelligence is the sharing of information

that alerts the analyst to "what is outside the normal security baseline and the risk", therefore allowing the analyst to take a proactive approach.

Threat intelligence is important, but the quality of the intelligence is vital in supporting the goals of information security. A variety of sources exist where organizations receive threat information and not all sources are created equal. One source of information is from government agencies, such as the Federal Bureau of Investigation and Homeland Security. These agencies provide credible information, but in most instances the information is not detailed because, as Participant 3 stated, "It's part of a criminal investigation and they don't want to reveal sources and methods". This information provided the organization with a direction to investigate, but unclear as to the actual problem.

The source of the threat intelligence plays a critical part in determining how effective the information is in support of situation awareness. The research data in the study revealed that organizations receive threat intelligence from a variety of sources and each has a certain level of quality, accuracy, and relevance. Not surprisingly, sources where paid subscriptions are utilized tend to have a higher level of quality and relevance to the organization than through free services or membership forums. Value is increased in obtaining intelligence from various sources even with the degree of quality. Gathering as much intelligence as possible and fusing the data provides the security analyst with identifying trends in the potential attack method and avenue of penetration into the network.

Summary

Chapter 4 provided insight into the importance of situation awareness and supported the research signifying an effective element within the security program for an organization. It is also acknowledged by the participants that based on individual experiences situation awareness is difficult to maintain and to improve its effectiveness should be supported by incorporating threat intelligence. Sources of threat intelligence vary in quality, accuracy and relevance and the participants agreed that this has an impact on the overall quality of the organization's security program.

Chapter 5 provides an interpretation of the findings in this study in addition to recommendations for further research. Implications for social change is discussed based on the data contained in the study is provided and the chapter concludes with a brief summary of the key essences of this research.

Chapter 5: Discussion, Conclusions, and Recommendations

Introduction

Threat intelligence is a vital security resource for advance knowledge of a potential cyber-attack and in determining the appropriate response. The purpose of this research study was to gain an understanding of the value threat intelligence provides to cyber situation awareness for the security analyst and in the decision-making process relating to cyber-attacks.

This study contributed to the literature relating to threat intelligence in support of cyber situation awareness and demonstrated that the sharing of intelligence allowed the analyst to focus on specific exploits and vulnerabilities that resulted in improved support in the decision-making process. Key findings of this study revealed that threat intelligence has the potential to improve the security posture of the organization and has the capability of supporting a proactive security process. The degree of improvement is the result of receiving advanced information from reliable sources capable of relaying accurate information of a potential attack. In addition, improvements in threat intelligence must be implemented that include increasing the level of specific details in relaying threats and improve information sharing processes between organizations.

Interpretation of Findings

This study's findings indicated that implementing a threat intelligence program may provide a complimentary component to a security analyst's cyber situation awareness. This study provided an increased understanding of the importance of the analyst's ability to perceive anomalies in an organization's network, understand the

meaning anomalies may have in regard to information security, and to project the consequences.

Research Question 1: Effectiveness of Situation Awareness

The first research question was to examine the effectiveness of the analyst's ability to understand the changes and determine the appropriate response to a cyber-attack based in cognitive situation awareness. The research data in this study revealed a certain level of effectiveness in situation awareness in response to cyber-attacks. The security analyst receives information pertaining to the activities on the network from various sources. Organizations implemented various types of security devices to detect and record in system logs events or activities that are examined on a regular basis. In addition, information is received from users, vendors, and/or other external entities about observed activities that appear to be abnormal but have not generated an alert to the security analyst.

Situation awareness is critical in identifying and forming the proper response to cyber-attacks. Security devices are dependent on what is known and what has been viewed in the past. Attackers are constantly improving the exploits to bypass the security devices and gain entrance to the core of the network. The security analyst may at times observe actions that have not been noticed before and have not caused an alert to be generated. The analyst must rely on situation awareness to know that this activity does not seem right even though the analyst may not have specific information. It is through the use of situation awareness that the analyst is able to filter through the actions and identify what is real and what is just noise, a potential risk or issue compared to typical

volume, and where to focus and whether additional exploits are present other than the initial point of attack. Individuals internal and external to the organization may report observed activity that is questionable but do not have the knowledge to compare the activity with normal activity. The information conveyed to the security analyst is important, and by exercising perception, comprehension, and projection of the event, the analyst is able to see the differences from the normal baseline and recognize anomalous behavior.

The research supported that in understanding these differences, the analyst may determine if the events will cause harm and potentially make the best decision for further action. This supported the research in the literature review of this study in that situation awareness is a state of human awareness based on a level of understanding the situation, comprehending the meaning, and the ability to project the future state of the environment in accordance with the goal of the individual (Endsley, 1994; Lambert, 2001). Regardless of the security defenses based on hardware and software solutions, situation awareness by the security analyst may be critical in the effectiveness of the organization's cyber security program.

Research Question 2: Threat Intelligence in Support of Situation Awareness

The second research question was to examine how threat intelligence supports situation awareness in response to cyber-attacks. The research data shows that effective situation awareness supported the security analyst in understanding the threat, its consequences, and appropriate action to be taken, but it is not a process that will provide

meaningful advanced information. In the cyber realm, advanced knowledge of an attack or potential attack is critical.

Threat intelligence is valuable as it is designed to provide advanced information so the security analyst can focus on specific areas that may be vulnerable to attack and determine if additional security measures should be implemented in the network prior to being exploited by the attacker. Intelligence gives the analyst an awareness of activities outside of the organization. The technical details (hashes, ip address, e-mail address) may change from one attack to another, but the same behavior may be observed within the organization's network. With this information, the security analyst is aware that a greater risk exists, the patterns and signatures that may be present, paths into the network that may be exploited, and steps that others have implemented to neutralize or minimize the threat. Threat intelligence adds value for the security analyst situation awareness as it shortens the process in determining an appropriate response. Utilizing fusion analysis in the intelligence process may allow the analyst to take different pieces of information and fuse them together to formulate situation awareness across the enterprise so that quick decisions are made to react to the threat.

Threat intelligence supports the analyst situation awareness and may add value to the overall security program for the organization. This position is consistent with the literature research where intelligence coupled with information from security devices provides the necessary information to formulate an immediate and effective response to threats (Biermann et al., 2009). Security devices alone do not have the necessary data to support situation awareness or potential threats as the devices report only the information

that is known (Kornmaier & Jaouen, 2014). The process of intelligence is essential as it supports obtaining an accurate awareness of the situation as well as an assessment of future developments based on threats, which is necessary in the decision-making process.

Research Question 3: Difficulty in Maintaining Situation Awareness

The third research question was to examine the difficulty in maintaining situation awareness for information security. The research data supported that due to the speed of Internet processing and volume of potential vulnerabilities, cyber-attacks make it difficult for the security analyst to maintain effective situation awareness.

Organizations continually grow in the number of data servers in order to maintain the vast amounts of data generated and received in the course of business operations. Each server maintains event logs that records activities by individuals as well as errors with hardware, software, and data communications just to name a few. Combined, these logs can generate billions of lines of events in any given month. Because of the vast amount, it is impossible for the security analyst to parse through this amount of data quick enough to comprehend the information that is available to provide an indicator of the risk that may be present coupled with changes in the normal behavior in the network. Comprehending this information is easy to discuss but difficult to put into practice. Many different systems are interacting together, and it is difficult to establish a baseline to measure the level of situation awareness. In addition, with attacks that may be slow and do not generate any alerts, the security analyst may not notice any specific pattern to indicate changes in behavior or even comprehend any specific threat activity against the network. Additional issues also impacts the effectiveness in that analyst does not have the

time to analyze all of the data that is generated by the systems. The analyst situation awareness is negatively affected as systems begin to generate large amounts of data for analysis at a higher rate of speed. The security analyst is not capable of keeping the same pace and may lose some of his situation awareness ability and miss indicators of a potential threat. The attackers have the same technology and are running malware against the same solutions. This approach allows the attackers to practice the launch of the attack and make any modifications necessary to increase the chances of success. This results in activities not rising to a level of generating an alert for anyone to take appropriate action.

The study supported that maintaining situation awareness is a difficult process and is consistent with the research data in the literature review. The amount of data presented for analysis by the security devices and the dynamic nature of the environment causes the decision-maker to be easily overwhelmed in attempting to gain the required level of cyber situation awareness. Attacks against organizational networks have increased through zero-day vulnerabilities, botnets, and distributed denial of service. Hacker tools are more sophisticated and have created an imbalance of capabilities between the attacker and the defender (Hernandez-Ardieta et al., 2013). The speed in which attacks occur are barely measurable as they occur at the speed of light (Clarke & Knake, 2010). The speed coupled with the amount of data to analyze may hinder the ability of the analyst to maintain the proper level of situation awareness to adequately support the security program.

Research Question 4: Effectiveness of Threat Intelligence

The fourth research question was to examine the effectiveness of threat intelligence in support of information security. The research data in this study supported that implementing threat intelligence capability in the information security program may provide an effective mechanism in achieving a more comprehensive understanding of what is occurring in addition to the information being presented by the internal systems. Receiving advanced knowledge of different threats that may affect the organization may provide the security analyst the information needed to monitor for events that otherwise may infiltrate the network.

The effectiveness of threat intelligence relies on the source and the level of detail that is provided by the source. Organizations receive intelligence feeds from various sources: subscription-based, forum memberships, or free security websites and newsletters. In many instances, threat intelligence feeds are received from a variety of sources by the organization but not all of these sources are created equally for reliability and accuracy. For example, searching the Internet for threat information isn't necessarily reliable and may even be questionable depending on the actual source. Forums, such as InfraGard, provide an increased level of reliability, but may not be accurate. In other words, it is possible where some specific details are not released to aid the organization, which hinders the strengthening of the security posture. This becomes even more problematic for the organization if the intelligence source is prohibited from providing meaningful and detailed intelligence due to the fear of jeopardizing a criminal investigation.

Intelligence data is received daily, but only one threat analysis in ten provide any actionable information. The results also indicated that according to the study's participants, 20% of the analyses will provide any actionable information. Access to meaningful data is hampered by the cost factor for participation in sharing groups. Many services that provide threat intelligence require a subscription or annual membership fee to receive information that is relevant to the organization. Not all services are created equally, and the threat intelligence provided vary in detail and quality. While the information provided is valuable, the cost may be prohibitive for some of the smaller companies.

Organizations are reluctant to provide detailed information relating to breaches of networks or potential attacks due to legal restrictions. One of the legal concerns pertains to respecting individuals' privacy so that the personal information is not released to other organizations. Various federal regulations protect the consumer's privacy through the Health Insurance Portability and Accountability Act (Centers for Disease Control and Prevention, U.S. Department of Health and Human Services, 2003), Payment Card Industry Data Security Standard (PCI Security Standards Council, n.d.) and others as governed through the Federal Trade Commission and the Federal Communications Commission to name a few.

The study supported that threat intelligence is important and has the potential to add value to the overall security program but has lacked in providing enough meaningful and consistent threat data that is needed for strengthening information security. Threat actors participate in knowledge sharing so malicious software and techniques can be

improved. The information shared through the black market contains results of previous exploits, updated applications to account for new technologies deployed, and knowledge of specific targets and the most vulnerable path into the network. One main reason these actors are successful is attributed to the sharing of intelligence. According to the participants in this study, organizations may need to follow the same approach in order to improve the effectiveness of threat intelligence capability, thereby increasing the effectiveness of the overall security posture.

Summary

Research indicated that effective situation awareness is vital in order for the security analyst to understand any changes within the network, what these changes mean and the consequences of these changes towards the goal of information security. As technology evolves and speed of data transfer increases, the security analyst cannot rely solely on his situation awareness ability to discover a potential cyber-attack against the organization. The security analyst cannot always rely on the security devices to provide meaningful information as these devices can only alert to issues in which it has knowledge. Hackers use the same technology and security processes and continually adapt malicious software to by-pass the devices. While improvements in knowledge sharing are necessary and should be implemented, threat intelligence may add value to the security program by providing a focused view of the potential exploit, vulnerability and motivation behind the cyber-attack to support a more proactive and informed decision-making process.

Limitations of the Study

The research study was designed to draw on the technical knowledge and experiences of information or network security personnel. One limitation was based on the questions presented and the answers provided by the participant. In answering questions related to processes and other actions taken in the event of a breach, it was possible that the participant provided answers as a combination of various organizations he or she has been employed and not necessarily the current organization. In addition, differences were noted in the participants meaning of cyber situation awareness and the processes. It was possible that this difference may not have reflected some of the actual steps involved in the decision-making process. A second limitation was the reluctance of providing specific details as to the actual breach and the actual process undertaken to remediate the action. The reason may be due to the specific information being considered confidential and some critical details were omitted from the interview.

Recommendations for Further Study

Recommendations for further research were grounded in the strengths and limitations of this research study as well as the literature reviewed in Chapter 2. Cyber-attacks continue to penetrate organizations' data infrastructure by developing sophisticated

Further research may be directed towards the various types or sources for cyber intelligence. Incorporating a threat intelligence process to compliment the organization's information security program may provide an additional layer of security, but differences exists depending on the source. Several reasons may be discussed that reveal why

organizations choose a specific source and may uncover any relation between available sources for threat intelligence and the organization's decision not to participate. Understanding the differences in subscription services, security forums, and free services also may provide insight into the accuracy and reliability needed to strengthen the information security program.

Further research may be valuable in studying issues that hinder organizations in establishing an information sharing group with other organizations that are like in size, operate in the same industry, or have similar concerns regarding the protection of data. While this study did not concentrate in this area, organizations may have a reluctance in sharing information as to the current security processes and any details about a breach or potential breach of the infrastructure. This type of threat intelligence has the potential to be of value to others in that the information can be specific enough to take action or increase monitoring for any exploit.

Further research may be valuable through a quantitative approach to examine the relationship between the two variables of cyber threats and cyber intelligence. The data can be used to determine any cause and effect and to make predictions. A quantitative approach may also provide numerical data that can be analyzed statistically to examine any correlation between a proactive security approach to cyber threats and cyber intelligence.

Another area for further research may address the legal aspect of acquiring and sharing threat intelligence with other organizations. A limited number of knowledge sharing groups exist and the information provided may be restrictive so as to avoid

violating federal regulations and to avoid the appearance of collusion within a specific industry. Relaxing of some of the restrictions have occurred, but it is unsure as to whether it is enough and if organizations are gaining confidence in sharing information.

Implications

The conclusion of this research study offered implications for positive social change at the organizational level in the field of information security. Threats and attacks designed to infiltrate the organization's network security defenses are increasing in speed and sophistication. Traditional security techniques and devices are necessary elements but provide minimal security defenses. Security analysts continue to rely on event logs and automated alerts to gain an understanding of the threats and identify potential breaches. Using this information the decision-maker comprehends the event that is occurring and project the consequences of this action in order to determine the appropriate response. For many organizations, logs and alerts are the standard processes for monitoring the network for any potential threat or potential breach.

The value of this study showed that continuing the current security process is supporting a reactive approach to protecting the information contained within the organization's network. Continuing a reactionary process may hinder the ability of the organization to effectively protect the network and data. Security processes that incorporate a threat intelligence program may add value to the security analysts' situation awareness by focusing on specific potential vulnerabilities and determining whether appropriate security measures are implemented. These measures may include up to date patches for applications, additional rulesets for intrusion detection/protection systems and

firewalls. Additionally, threat intelligence identifies the method of attacks and motivation of the attacker and procedures to protect against the attack are provided and supports the analyst ability to focus on specific measures.

Organizations may add value to the security program through the implementation of a threat intelligence program. Participating in the sharing of knowledge about perceived and actual breaches within a controlled and trusted forum may improve the capabilities of identifying and remediating the threat through a proactive security posture.

Conclusions

This research study was designed to explore the overall value of threat intelligence in support of the security analyst cognitive situation awareness to support information security. The key points discovered during this study are:

1. Situation awareness is an ability of the security analyst that is necessary to support the organization's security program.
2. Due to the nature and speed of changes in attack postures and network defenses, effective situation awareness is difficult to maintain.
3. Threat intelligence may actively support the security analyst's situation awareness by providing advance information into the techniques and motivation of the attacker.
4. Threat intelligence provides the potential for the security analyst to focus on a vulnerability that may otherwise have not been examined.
5. Threat intelligence is effective in supporting information security, but requires more maturity as a process.

The primary process of information security relies on the traditional methods to alert the security analyst of any active or potential breach in the network security defenses. The traditional methods including the review of server event logs, intrusion detection systems and firewall alerts play a minimal but important part for security but can only relay information the devices know either at the time of the event or after the event has occurred in the network. A limitation to the current process is understanding the motive and goal of the attacker in advance of the potential breach. This method of information security is reactive by nature and causes the security analyst to react without the necessary information to adequately make an informed decision to the appropriate response.

The normal methods and procedures need to change to a more advantageous approach by implementing threat intelligence as part of the security process. Threat intelligence still requires more maturity in the consistency of the information and mechanism of distributing the information, confidence of organizations to share information as approach during and after a cyber-attack to trusted partners. Threat intelligence has the potential to provide the security analyst with advanced information from other organizations and government agencies as to the vulnerabilities, methods, and motivation of the attacker. Threat intelligence may be a means where the analyst may not need to only rely on what the organization has experienced, but the experiences of others and allows the analyst to focus on the specific nature of the attack before the event. Incorporating threat intelligence into the organizations' security program may begin to shift the protection mode from reactive to a proactive process.

References

Adeyinka, O. (2008). Internet Attack Methods and Internet Security Technology. In *Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on* (pp. 77–82). Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4530455

AlHogail, A., & Berri, J. (2012). Enhancing IT security in organizations through knowledge management. In *2012 International Conference on Information Technology and e-Services (ICITeS)* (pp. 1–6). https://doi.org/10.1109/ICITeS.2012.6216677

Baker, W. H., & Wallace, L. (2007). Is information security under control?: Investigating quality in information security management. *Security & Privacy, IEEE*, *5*(1), 36–44.

Baker, W., Hutton, A., Hylender, C. D., Pamula, J., Porter, C., & Spitler, M. (2012). Data Breach: Investigations Report, A study conducted by the Verizon RISK Team with co-operation from the US Secret Service and the Dutch High-Tech Crime Unit. *As Of*, *17*.

Barford, P., Dacier, M., Dietterich, T. G., Fredrikson, M., Giffin, J., Jajodia, S., … Ning, P. (2010). Cyber SA: Situational awareness for cyber defense. In *Cyber Situational Awareness* (pp. 3–13). Springer. Retrieved from http://link.springer.com/content/pdf/10.1007/978-1-4419-0140-8_1

Barnum, S. (2012). Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX™). *MITRE Corporation*, *11*.

Retrieved from http://trafficlight.bitdefender.com/info?url=http%3A//www.standardscoordination.org/sites/default/files/docs/STIX_Whitepaper_v1.1.pdf&language=en_US

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *The Qualitative Report*, *13*(4), 544–559.

Beer, P. D., & von Solms Basie, S. (2013). The case for cyber counterintelligence. In *Adaptive Science and Technology (ICAST), 2013 International Conference on* (pp. 1–8). IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6707493

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The case research strategy in studies of information systems. *MIS Quarterly*, 369–386.

Biermann, J., Hörling, P., & Snidaro, L. (2009). Automated Support for Intelligence in Asymmetric Operations: Requirements and Experimental Results. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.157.2542&rep=rep1&type=pdf

Bosworth, S., Kabay, M. E., & Whyne, E. (2012). *Computer Security Handbook*. John Wiley & Sons.

Boyd, J. R. (1987a). *Destruction and creation*. US Army Comand and General Staff College. Retrieved from http://goalsys.com/books/documents/DESTRUCTION_AND_CREATION.pdf

Boyd, J. R. (1987b). Organic design for command and control. *A Discourse on Winning and Losing*. Retrieved from http://www.dnipogo.org/boyd/organic_design.pdf

Boyd, J. R. (1987c). The Strategic Game of? and? *Slideshow. URL: Http://Dni. Net/Boyd/Strategic_game. Pdf [Online*. Retrieved from http://www.evenmere.org/~bts/Random-Collected-Documents/Boyd/The%20Strategic%20Game.pdf

Boyd, J. R. (1996). The essence of winning and losing. *Unpublished Lecture Notes*. Retrieved from http://tobeortodo.com/wp-content/uploads/2011/11/essence_of_winning_losing.pdf

Boyd, J. R., Richards, C. W., Spinney, F. C., & Richards, G. G. (2007). *Patterns of conflict*. Defense and the National Interest. Retrieved from http://www.projectwhitehorse.com/pdfs/boyd/patterns%20of%20conflict.pdf

Brewer, R. (2014). Advanced persistent threats: minimising the damage. *Network Security*, *2014*(4), 5–9. https://doi.org/10.1016/S1353-4858(14)70040-6

Brumley, L., Kopp, C., & Korb, K. (2006). The Orientation step of the OODA loop and Information Warfare. In *Information Warfare and Security Conference* (p. 20). Retrieved from http://conferences.ecu-sri.org/proceedings/2006/iwar/Proceedings_IWAR_2006.pdf#page=26

Bryant, D. J. (2006). Rethinking OODA: Toward a Modern Cognitive Framework of Command Decision Making. *Military Psychology (Taylor & Francis Ltd)*, *18*(3), 183–206. https://doi.org/10.1207/s15327876mp1803_1

Carroll, L. (1992). *Desperately seeking SA*. DTIC Document. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA531172

Charmaz, K. (2014). *Constructing grounded theory*. Sage.

Chism, N. V. N., Douglas, E., & Hilson, W. (2008). Qualitative research basics: A guide for engineering educators. *National Science Foundation2008*. Retrieved from http://adrge.engin.umich.edu/wp-content/uploads/sites/7/2013/06/Chism-Douglas-Hilson-Qualitative-Research-Basics-A-Guide-for-Engineering-Educators.pdf

Chu, S.-Y. (2013). Internet, Economic Growth and Recession. *Modern Economy*, *4*(3A special issue), 209–213.

Clarke, R. A., & Knake, R. K. (2010). *Cyber war*. New York, NY: Harper Collins.

Cole, E. (2011). *Network Security Bible* (2nd ed.). Indianapolis, IN: John Wiley & Sons.

Conklin, A., & Dietrich, G. (2008). Systems theory model for information security. In *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual* (pp. 265–265). Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4438970

Control, C. for D., Prevention, & others. (2003). HIPAA privacy rule and public health. Guidance from CDC and the US Department of Health and Human Services. *MMWR: Morbidity and Mortality Weekly Report*, *52*(Suppl. 1), 1–17.

Creswell, J. W. (2007). *Qualitative inquiry and research design*. SAGE.

Cummings, M. L., Bruni, S., & Mitchell, P. J. (2010). Human Supervisory Control Challenges in Network-Centric Operations. *Reviews of Human Factors and Ergonomics*, *6*(1), 34–78. https://doi.org/10.1518/155723410X12849346788660

Cyril, O. (2012). *Situational Awareness in Computer Network Defense: Principles, Methods and Applications: Principles, Methods and Applications*. IGI Global.

Dalrymple, M., & Schiflett, S. (1997). Measuring situational awareness of AWACS weapons directors. In *Situational awareness in the tactical air environment (SOAR 97-01). Proceedings of the Naval Air Warfare Center's First Annual Symposium at Patuxent River, MD. WPAFB, OH: CSERIAC*.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, *4*(2), 92–100.

Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2009). Information security: The moving target. *Computers & Security*, *28*(3–4), 189–198. https://doi.org/10.1016/j.cose.2008.11.007

Doupé, A., Egele, M., Caillat, B., Stringhini, G., Yakin, G., Zand, A., … Vigna, G. (2011). Hit'em where it hurts: a live security exercise on cyber situational awareness. In *Proceedings of the 27th Annual Computer Security Applications Conference* (pp. 51–61). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=2076740

DSS, P. (2014). *Payment Card Industry Data Security Standards*. Abril. Retrieved from http://trafficlight.bitdefender.com/info?url=http%3A//umanitoba.ca/admin/financial_services/media/PCI_DSS_Compliance_FinalNov_01_-_PDF.pdf&language=en_US

Dutt, V., Ahn, Y.-S., & Gonzalez, C. (2011). Cyber situation awareness: Modeling the security analyst in a cyber-attack scenario through instance-based learning. *Data and Applications Security and Privacy XXV*, 280–292.

Endsley, M., & Jones, W. M. (1997). *Situation Awareness Information Dominance & Information Warfare.* DTIC Document. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA347166

Endsley, M. R. (1988a). Design and evaluation for situation awareness enhancement. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 32, pp. 97–101). SAGE Publications. Retrieved from http://pro.sagepub.com/content/32/2/97.short

Endsley, M. R. (1988b). Situation awareness global assessment technique (SAGAT). In *Aerospace and Electronics Conference, 1988. NAECON 1988., Proceedings of the IEEE 1988 National* (pp. 789–795). IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=195097

Endsley, M. R. (1994). Situation Awareness in Dynamic Human Decision Making: Theory. *Situation Awareness for Complex System Operations*, 27.

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *37*(1), 32–64.

Endsley, M. R. (2000). Situation models: An avenue to the modeling of mental models. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 44, pp. 61–64). SAGE Publications. Retrieved from http://pro.sagepub.com/content/44/1/61.short

Endsley, M. R. (2001). Designing for situation awareness in complex systems. In *Proceedings of the Second International Workshop on symbiosis of humans, artifacts and environment*.

Endsley, M. R. (2012). *Designing for Situation Awareness: An Approach to User-Centered Design, Second Edition*. CRC Press.

Etsebeth, V. (2011). Defining the Current Corporate IT Risk Landscape. *Journal of International Commercial Law & Technology*, *6*(2), 62–73.

Farahmand, F., Navathe, S. B., Sharp, G. P., & Enslow, P. H. (2005). A Management Perspective on Risk of Security Threats to Information Systems. *Information Technology and Management*, *6*(2–3), 203–225. https://doi.org/http://dx.doi.org.ezp.waldenulibrary.org/10.1007/s10799-005-5880-5

Farhadi, M., Ismail, R., & Fooladi, M. (2012). Information and Communication Technology Use and Economic Growth: e48903. *PLoS One*, *7*(11). https://doi.org/http://dx.doi.org.ezp.waldenulibrary.org/10.1371/journal.pone.0048903

Faysel, M. A., & Haque, S. S. (2010). Towards cyber defense: research in intrusion detection and intrusion prevention systems. *IJCSNS International Journal of Computer Science and Network Security*, *10*(7), 316–325.

Fernandez Vazquez, D., Pastor Acosta, O., Brown, S., Reid, E., & Spirito, C. (2012). Conceptual framework for cyber defense information sharing within trust relationships. In *Cyber Conflict (CYCON), 2012 4th International Conference on*

(pp. 1–17). IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6243990

FIPS, P. (2006). *200 FEDERAL INFORAMTION PROCESSES STANDARDS PUBLICATION–Minimum Security Requirements for Federal Information and Information Systems*. March.

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness – A systematic review of the literature. *Computers & Security*, *46*, 18–31. https://doi.org/10.1016/j.cose.2014.06.008

Gendron, A., & Rudner, M. (2012). Assessing Cyber Threats to Canadian Infrastructure. *Occasional Papers*, *2012*, 10–01.

Gibson, W. (1984). Neuromancer. *Ace*, *9*.

Grant, T., & Kooter, B. (2005). Comparing OODA & other models as Operational View C2 Architecture Topic: C4ISR/C2 Architecture. In *10th International Command and Control Research and Technology Symposia (ICCRTS)*. Retrieved from http://re.vu/doc-download/bmkooter/176014/work_example-bas.kooter-comparingoodaabstract.285187.1350938508.pdf

Green, J., & Thorogood, N. (2013). *Qualitative methods for health research*. Sage.

Haass, J. C., Ahn, G.-J., & Grimmelmann, F. (2015). ACTRA: A Case Study for Threat Information Sharing. In *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security* (pp. 23–26). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=2808135

Hammond, G. T. (2013). Reflections on the Legacy of John Boyd. *Contemporary Security Policy*, *34*(3), 600–602.

Hasík, J. (2013). Beyond the Briefing: Theoretical and Practical Problems in the Works and Legacy of John Boyd. *Contemporary Security Policy*, *34*(3), 583–599.

Hernandez-Ardieta, J. L., Tapiador, J. E., & Suarez-Tangil, G. (2013). Information sharing models for cooperative cyber defence. In *2013 5th International Conference on Cyber Conflict (CyCon)* (pp. 1–28).

Hurley, M. M. (2012). For and from Cyberspace: Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance. *Air & Space Power Journal*, *26*(6), 12–33.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, *1*, 80.

Jajodia, S., Liu, P., Swarup, V., & Wang, C. (Eds.). (2009). *Cyber Situational Awareness: Issues and Research* (1st ed.). Springer.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Jones, R. E. T., Connors, E. S., & Endsley, M. R. (2011). A framework for representing agent and human situation awareness. In *2011 IEEE First International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)* (pp. 226–233). https://doi.org/10.1109/COGSIMA.2011.5753450

Jumratjaroenvanit, A., & Teng-amnuay, Y. (2008). Probability of Attack Based on System Vulnerability Life Cycle (pp. 531–535). Presented at the International Symposium on Electronic Commerce and Security, IEEE. https://doi.org/10.1109/ISECS.2008.212

Kaplan, B., & Maxwell, J. A. (2005). Qualitative research methods for evaluating computer information systems. In *Evaluating the organizational impact of healthcare information systems* (pp. 30–55). Springer. Retrieved from http://link.springer.com/chapter/10.1007/0-387-30329-4_2

Kim, W., Jeong, O.-R., Kim, C., & So, J. (2011). The dark side of the Internet: Attacks, costs and responses. *Information Systems*, *36*(3), 675–705. https://doi.org/10.1016/j.is.2010.11.003

Kim, Y. (2011). The pilot study in qualitative inquiry: Identifying issues and learning lessons for culturally competent research. *Qualitative Social Work*, *10*(2), 190–206.

Kissel, R. (2013). Glossary of key information security terms. *NIST Interagency Reports NIST IR*, *7298*, 3.

Koch, R., Stelte, B., & Golling, M. (2012). Attack trends in present computer networks. In *Cyber Conflict (CYCON), 2012 4th International Conference on* (pp. 1–12). IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6243980

Kornmaier, A., & Jaouen, F. (2014). Beyond technical data - a more comprehensive situational awareness fed by available intelligence information. In *Cyber Conflict*

(CyCon 2014), 2014 6th International Conference On (pp. 139–154). https://doi.org/10.1109/CYCON.2014.6916400

Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. *Cyberpower and National Security*, 26–28.

Kumar, G., & Kumar, K. (2014). Network security–an updated perspective. *Systems Science & Control Engineering: An Open Access Journal*, *2*(1), 325–334.

Lambert, D. A. (2001). Situations for situation awareness. *Proc. of Fusion 2001*. Retrieved from http://ftp.isif.org/fusion/proceedings/fusion01CD/fusion/searchengine/pdf/ThC22.pdf

Loveland, G., & Lobel, M. (2011). Eye of the storm: Key findings from the 2012 global state of information security survey. *Pricewaterhouse Coopers LLP*.

Lukasik, S. J. (2011). Why the Arpanet Was Built. *IEEE Annals of the History of Computing*, *33*(3), 4–21. https://doi.org/10.1109/MAHC.2010.11

Luokkala, P., & Virrantaus, K. (2014). Developing information systems to support situational awareness and interaction in time-pressuring crisis situations. *Safety Science*, *63*, 191–203.

Marra, W., & McNeil, S. (2013). Understanding'The Loop': Regulating the Next Generation of War Machines. *Harvard Journal of Law and Public Policy*, *36*(3). Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2043131

Mattern, T., Felker, J., Borum, R., & Bamford, G. (2014). Operational Levels of Cyber Intelligence. *International Journal of Intelligence and CounterIntelligence*, *27*(4), 702–719.

Maxwell, J. A. (2005). *Qualitative Research Design* (2nd ed., Vol. 42). Sage Publications. Retrieved from http://sutlib2.sut.ac.th/sut_contents/H94621.pdf

Mendyk-Krajewska, T., & Mazur, Z. (2010). Problem of network security threats. In *2010 3rd Conference on Human System Interactions (HSI)* (pp. 436–443). https://doi.org/10.1109/HSI.2010.5514533

Merriam, S. B., & others. (2002). Introduction to qualitative research. *Qualitative Research in Practice: Examples for Discussion and Analysis*, *1*, 1–17.

Mets, D. R. (2004). Boydmania. *Air and Space Power Journal*, *18*, 98–108.

Mihailovic, A., Chochliouros, I. P., Georgiadou, E., Spiliopoulou, A. S., Sfakianakis, E., Belesioti, M., … Alonistioti, N. (2009). Situation awareness mechanisms for cognitive networks. In *International Conference on Ultra Modern Telecommunications Workshops, 2009. ICUMT '09* (pp. 1–6). https://doi.org/10.1109/ICUMT.2009.5345485

Miles, M. B., & Huberman, A. M. (1994). *Qualitative Data Analysis: An Expanded Sourcebook*. SAGE Publications.

Miller, A. (2006). Situational awareness – from the battlefield to the corporation. *Computer Fraud & Security*, *2006*(9), 13–16. https://doi.org/10.1016/S1361-3723(06)70420-1

Oliverio, J., Masakowski, Y. R., Beck, H., & Appuswamy, R. (2007). ISAS: a human-centric digital media interface to empower real-time decision-making across distributed systems. In *Proceedings of the twelfth international conference on 3D web technology* (pp. 81–87). New York, NY, USA: ACM. https://doi.org/10.1145/1229390.1229403

Onwubiko, C. (2009). Functional requirements of situational awareness in computer network security. In *Intelligence and Security Informatics, 2009. ISI '09. IEEE International Conference on* (pp. 209–213). https://doi.org/10.1109/ISI.2009.5137305

Osinga, F. (2013). Getting'A Discourse on Winning and Losing: A Primer on Boyd's 'Theory of Intellectual Evolution. *Contemporary Security Policy*, *34*(3), 603–624.

Pace, P. (2006). National Military Strategy for Cyberspace Operations. *Unclassified Memo, December*.

Patton, M. Q. (2002). *Qualitative Research & Evaluation Methods*. SAGE Publications.

Philp, W. R., & Martin, C. P. (2009). A philosophical approach to time in military knowledge management. *Journal of Knowledge Management*, *13*(1), 171–183.

Polk, R. B. (2000). A Critique of the Boyd Theory - Is it Relevant to the Army? *Defense Analysis*, *16*(3), 257–276. https://doi.org/10.1080/07430170020016270

Ponemon Institute. (2014, April). "Exposing the cybersecurity cracks" - Google Search. Retrieved October 18, 2015, from https://www.google.com/?gws_rd=ssl#q=%22Exposing+the+cybersecurity+cracks%22

Ponemon Institute. (2015, November 15). Exchanging cyber threat intelligence there has to be a better way. Retrieved April 3, 2016, from http://www.ponemon.org/blog/the-second-annual-study-on-exchanging-cyber-threat-intelligence-there-has-to-be-a-better-way

Ponemon Institute. (2012). 2012 Cost of Cyber Crime Study. Retrieved May 25, 2013, from http://www.ponemon.org/library/2012-cost-of-cyber-crime-study

Potts, M. (2012). The state of information security. *Network Security*, *2012*(7), 9–11. https://doi.org/10.1016/S1353-4858(12)70064-8

Rattray, G. J. (2001). *Strategic warfare in cyberspace*. MIT press. Retrieved from http://books.google.com/books?hl=en&lr=&id=lVbQ4AxfYaMC&oi=fnd&pg=PP1&dq=Strategic+warfare+in+cyberspace&ots=OHz7nCQJlD&sig=3JLTtAS54D2IrKNdeytS_WcmFUc

Richardson, R. (2010). *2011 CSI computer crime and security survey," 2011*.

Ritchie, J., Lewis, J., Nicholls, C. M., & Ormston, R. (2013). *Qualitative research practice: A guide for social science students and researchers*. Sage.

Rosli, D. I., Rahma, A. A., & Alias, R. A. (2011). Situational Awareness needs for system interaction design. In *2011 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)* (pp. 1888–1892). https://doi.org/10.1109/IEEM.2011.6118243

Salerno, J., Hinman, M., Boulware, D., & Bello, P. (2003). *Information Fusion for Situational Awareness*.

Salfinger, A., Retschitzegger, W., & Schwinger, W. (2013). Maintaining Situation Awareness over Time–A Survey on the Evolution Support of Situation Awareness Systems. In *Technologies and Applications of Artificial Intelligence (TAAI), 2013 Conference on* (pp. 274–281). IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6783881

Samuels, M. (2014). Friction, Chaos and Order (s): Clausewitz, Boyd and Command Approaches. *Journal of Military and Strategic Studies*, *15*(4). Retrieved from http://www.jmss.org/jmss/index.php/jmss/article/view/571

Sarter, N. B., & Woods, D. D. (1991). Situation awareness: A critical but ill-defined phenomenon. *The International Journal of Aviation Psychology*, *1*(1), 45–57.

Schneider, D. (2012). The state of network security. *Network Security*, *2012*(2), 14–20. https://doi.org/10.1016/S1353-4858(12)70016-8

Schwartau, W. (1994). *Information warfare: Chaos on the electronic superhighway*. Thunder's Mouth Press. Retrieved from http://dl.acm.org/citation.cfm?id=528243

Sharp, W. G. (1999). *Cyberspace and the Use of Force*. Aegis Research Corporation. Retrieved from http://dl.acm.org/citation.cfm?id=520562

Sigholm, J., & Bang, M. (2013). Towards Offensive Cyber Counterintelligence: Adopting a Target-Centric View on Advanced Persistent Threats. In *Intelligence and Security Informatics Conference (EISIC), 2013 European* (pp. 166–171). IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6657147

Stake, R. E. (2013). *Multiple case study analysis*. Guilford Press. Retrieved from http://trafficlight.bitdefender.com/info?url=https%3A//books.google.com/books%3Fhl%3Den%26lr%3D%26id%3DrQWT5aDHiZYC%26oi%3Dfnd%26pg%3DPT21%26dq%3Dcase+study%26ots%3DIFmXDvKuui%26sig%3DhSaXnbvaQJI_lm4_9jP_2hOwwPg&language=en_US

Standardization, I. O. for, & Commission, I. E. (2005). ISO/IEC 27001: 2005. *Information Technology–security Techniques–information Security Management Systems–requirements*.

Tadda, G. P. (2008). Measuring performance of Cyber situation awareness systems. In *Information Fusion, 2008 11th International Conference on* (pp. 1–8).

Tamjidyamcholo, A., Bin Baba, M. S., Shuib, N. L. M., & Rohani, V. A. (2014). Evaluation model for knowledge sharing in information security professional virtual community. *Computers & Security*, *43*, 19–34. https://doi.org/10.1016/j.cose.2014.02.010

Tenney, Y. J., & Pew, R. W. (2006). Situation Awareness Catches On: What? So What? Now What? *Reviews of Human Factors and Ergonomics*, *2*(1), 1–34. https://doi.org/10.1177/1557234X0600200102

Tyworth, M., Giacobe, N. A., Mancuso, V., & Dancy, C. (2012). The distributed nature of cyber situation awareness. In *2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)* (pp. 174–178). https://doi.org/10.1109/CogSIMA.2012.6188375

Updegrove, A. (2011). Cyber Security and the Vulnerability of Networks: Why we Need to Rethink our Cyber Defenses Now. *Standards Today*, *10*(1), 7–35.

Verizon. (2013, April 13). 2013 Data Breach Investigations Report. Retrieved May 17, 2013, from http://www.verizonenterprise.com/DBIR/2013/

Vidulich, M. A. (1995). The role of scope as a feature of situation awareness metrics. In *Proceedings of the International Conference on Experimental Analysis and Measurement of Situation Awareness* (pp. 69–74).

von Solms, R., & van Niekerk, J. (n.d.). From information security to cyber security. *Computers & Security*. https://doi.org/10.1016/j.cose.2013.04.004

White House. (2006). United States National Security Presidential Directive 54. *Homeland Security Presidential Directive*, *23*.

Whitman, M. E., & Mattord, H. J. (2010). *Principles of Information Security*. Cengage Learning.

Wickens, C. D. (2008). Situation awareness: Review of Mica Endsley's 1995 articles on situation awareness theory and measurement. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *50*(3), 397–403.

Yang, S. J., Byers, S., Holsopple, J., Argauer, B., & Fava, D. (2008). Intrusion activity projection for cyber situational awareness. In *Intelligence and Security Informatics, 2008. ISI 2008. IEEE International Conference on* (pp. 167–172). https://doi.org/10.1109/ISI.2008.4565048

Yin, R. K. (2009). *Case Study Research: Design and Methods*. SAGE.

Appendix A: Letter of Invitation

Dear ___,

My name is Billy Paul Gilliam and I am a doctoral candidate in the Management and Technology Department at Walden University. I am conducting a research study as part of the requirements of my degree in Information Systems Management and I would like to invite you to participate.

I am studying the value of cyber intelligence information sharing in support of situation awareness on the part of the security professional. Situation awareness is the process in perceiving changes in a computer network, comprehending the meaning of these changes, and projecting the effects of these changes in the future. For this study, changes are described as attacks against the network, regardless if the attack is successful or not.

The study will be conducted in an interview session lasting approximately one hour. There is the possibility that a follow up interview may be necessary to resolve any questions or to clarify any comments. To insure accuracy of the conversation, an audio recording may be made and used in the transcription of the interview. In addition, you will have the opportunity to review the written notes to verify its accuracy.

To be a participant, the inclusion criteria is: at least 5 years direct experience in information security; current role within your organization must be in information security; direct technical experience with network defense to include firewalls, routers, intrusion detection, and security event analysis.

I will be happy to answer any questions you have about the study. You may contact me at xxx-xxx-xxxx or email billy.gilliam@waldenu.edu.

If you believe you meet the criteria and decide to participate, I will forward a letter of consent for you to review that outlines the specific process of this study as well as other contact information should you have any additional questions or concerns.

Thank you for your consideration.

With kind regards,

Billy Gilliam

Appendix B: Additional Interview Questions

Describe how you were alerted to this incident?

How much time did it take to remediate the incident?

Describe any additional investigations performed related to the incident after remediation?

What factors were included in your decision making to respond to this incident?

What sources do you rely on to keep abreast of the latest security threats?

Are you a member of any cybersecurity information sharing groups? If not, why?

How effective is your participation with cyber intelligence information sharing in your organization's information security program?

How accurate is the information you receive relating to the latest threats?

With several servers generating various event logs and a high number of alerts, how do you monitor them to identify any real or significant incidents?

Do you believe the analyst is able to do an adequate job in analyzing and determining what events are going on?

Describe the reasons for participating in cyber information sharing groups.

Do you believe that threat intelligence could have minimized or prevented the consequences of your incident? Why or why not?

Describe the main elements of a cyber intelligence information sharing program that would be (or is) most important to you.