2016

Exploring the Cybersecurity Hiring Gap

Adam O. Pierce
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Adam Pierce

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. Carol-Anne Faint, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Cheryl Lentz, Committee Member, Doctor of Business Administration Faculty

Dr. Alen Badal, University Reviewer, Doctor of Business Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2016

Abstract

Exploring the Cybersecurity Hiring Gap

by

Adam O. Pierce

MBA, Walden University, 2011

MS, Keller Graduate School of Management, 2009

BA, Old Dominion University, 2002

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

December 2016

Abstract

Cybersecurity is one of the fastest growing segments of information technology. The Commonwealth of Virginia has 30,000 cyber-related jobs open because of the lack of skilled candidates. The study is necessary because some business managers lack strategies for hiring cybersecurity professionals for U.S. Department of Defense (DoD) contracts. The purpose of this case study was to explore strategies business managers in DoD contracting companies used to fill cybersecurity positions. The conceptual framework used for this study was the organizational learning theory. A purposeful sample of 8 successful business managers with cybersecurity responsibilities working for U.S. DoD contracting companies that successfully hired cybersecurity professionals in Hampton Roads, VA participated in the study. Data collection included semistructured interviews and a review of job postings from the companies represented by the participants. Coding, content, and thematic analysis were the methods used to analyze data. Within-methods triangulation was used to add accuracy to the analysis. At the conclusion of the data analysis, two main themes emerged: maintaining contractual requirements and a strong recruiting process. Contractual requirements guided how hiring managers hired cybersecurity personnel and executed the contract. A strong hiring process added efficiency to the hiring process. The findings of the study may contribute to positive social change by encouraging the recruitment and retention of cybersecurity professionals. Skilled cybersecurity professionals may safeguard businesses and society from Internet crime, thereby encouraging the safe exchange and containment of data.

Exploring the Cybersecurity Hiring Gap

by

Adam O. Pierce

MBA, Walden University, 2011

MS, Keller Graduate School of Management, 2009

BA, Old Dominion University, 2002

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

December 2016

Dedication

I dedicate my study to those with hopes, dreams and fears of achieving the highest level of education. This is a testament that you can do it.

Acknowledgments

I give thanks to the Almighty for all he has done for me. To my wife and my kids, thank you for enduring the struggle with me. You have kept me accountable at every turn, and for that, I am grateful. To my parents, thank you for the inspiration and encouragement. You always said I could do it. To Dr. Faint, thank you for all of your kind words, corrections, and your encouragement. You have been the best mentor any student could ask for.

Table of Contents

List of Tables

Section 1: Foundation of the Study

Cybersecurity is a major concern for governments and private companies around the world (Dunn Cavelty, 2014). Cybersecurity is also one of the fastest growing segments of Information Technology (IT); however, businesses have a small quantity of qualified cyber security professionals to fill the positions necessary to address security concerns (Suby & Dickson, 2015). The cyber security professionals responsible for implementing information security fail to align business objectives with proper security objectives to protect the organization’s data (Jirasek, 2012).

Background of the Problem

Cybersecurity professionals protect information systems and facilities, and provide training for the organization’s users (von Solms & van Niekerk, 2013a). In an investigation data breach report provided by the Verizon Risk Team, outsiders perpetrated 92% of the 855 incidents investigated by team (Verizon Risk Team, 2012). The Verizon Risk Team report also documented 276 of the 855 incidents happened because of weak or stolen user credentials (Verizon Risk Team, 2012). Eighty-one percent of the 855 investigated attacks involved some form of hacking (Verizon Risk Team, 2012).

A Bloomberg government survey of 172 Fortune 500 companies discovered that the companies surveyed spent $5.3 billion a year on IT security (Garfinkel, 2012). Despite the amount of money spent, the rate of successfully stopping attacks was 69% (Garfinkel, 2012). Understanding how to prevent outsiders from penetrating the network and maintaining the functionality of information systems resources are critical parts of a cybersecurity professional’s job. Understanding how the cybersecurity position fits into the overall IT strategy for the organization is equally important (Jirasek, 2012). To conduct cybersecurity efficiently, cybersecurity professionals must receive extensive training in networking, systems administration, and the principles of information security (Podhorec, 2012). Cybersecurity professionals must understand the organization's mission and objectives to ensure that the organization’s cyber efforts align with the organization’s vision (Kolfal, Patterson, & Yeo, 2013).

Problem Statement

The Commonwealth of Virginia has 30,000 cyber-related jobs open because of the lack of skilled candidates (Day, 2014). In 2014, 54% of 17,227 cybersecurity job postings required at least one cybersecurity certification (Hughes, 2015). The general business problem is the vulnerability exposure caused by the severe shortage of trained cybersecurity professionals with the required knowledge, skills, and attributes to protect the organizations' information systems. This results in (a) loss of profits, (b) attacks on customer data, and (c) the disruption of networks essential to the economy (Clarke & Jackson, 2015). The specific business problem is that some business managers in the U.S. Department of Defense (DoD) contracting companies lack strategies to fill cybersecurity positions.

Purpose Statement

The purpose of this qualitative case study was to explore strategies business managers in U.S DoD contracting companies use to fill cybersecurity positions. The population used in the study included business managers working for U.S. DoD contracting companies with cybersecurity responsibilities in Hampton Roads, Virgnia. The geographical location of the study was within the area of southeastern Virginia in the United States.

I used purposeful sampling with a sample size of eight participants to gather data. The sample size may seem limited, but Robinson (2013) suggested that a sample size of three to 16 is ideal for small-scale, interview-based qualitative research. This study's contribution to social change is that it will provide organizations with an understanding of the best strategies they can use to fill cybersecurity positions with professionals who have the knowledge, skills, and attributes necessary to defend the organization's networks and information systems.

Nature of the Study

I conducted a qualitative case study to explore the strategies used to fill cybersecurity positions within the U.S. DoD contracting industry. The qualitative method is an academic research method that researchers use to gain an understanding of the subject of research (Chenail, 2011). The qualitative research method is used to understand a phenomenon (Yin, 2013).

In contrast, researchers use quantitative methods when there is a need to investigate current conditions, relationships of variables, and the cause and effect of certain phenomena (Mustafa, 2011; Oleinik, 2011). The purpose of this study was to explore the perceptions and experiences of business managers with cybersecurity position hiring responsibility for U.S. DoD contracting companies. A lack of survey instruments in the explored literature prevented the use of the quantitative method for this study. The quantitative method also did not align with the purpose of the study.

A mixed methods approach is a combination of the traditional qualitative and quantitative methodologies (Denzin, 2012; Venkatesh, Brown, & Bala, 2013). Mixed methods methodology did not align with this study because the intent of the study was to explore successful strategies used to hire cybersecurity professionals for DoD contracts, not to quantify the existence of this behavior.

The three qualitative research designs considered for the study were the phenomenological inquiry, ethnographic analysis, and case study analysis. In a phenomenological study, the researcher uses the lived experiences of a group of research participants to understand the concept or the phenomenon (Walker, 2012). There was no alignment between the phenomenological design and the intent of this study because the participant pool in one DoD contracting organization was not large enough to attract the 20 participants required for the study.

Ethnographic analysis requires the researcher to gather data to understand the cultural patterns of a group by becoming a part of the group (Petty, Thomson, & Stew, 2012). There was no alignment between the ethnographic approach and the intent of this study because the study did not seek to gain knowledge about the cultural patterns of cybersecurity professionals.

Case study research design provides an in-depth look at an individual or small participant pool, with an emphasis on exploration and description (Petty et al., 2012). According to Houghton et al. (2013), the case study design allows the researcher to have more flexibility in data collection. Houghton et al. posited that the researcher adapts accordingly to the data. A case study design best suited the research exploring hiring processes of cybersecurity recruitment and retention. The in-depth interviews and exploration of the job descriptions provided a deeper understanding of the processes and procedures necessary to hire successful cybersecurity professionals for DoD contracts.

I decided to use the case study research design for this study. The flexibility of the case study research design allowed me to capture information about the processes used by cybersecurity managers during the hiring process. Petty et al. (2012) posited that case study research design is appropriate if the focus of the research is to explore the events and behaviors that result in the occurrence of a certain condition. This study was an exploration of hiring practices for U.S. DoD contracting companies in Hampton Roads, Virginia. The case study method complimented the intent of the study and was the best method for use in the study because of the flexibility of the design and the small participation pool used in the study.

Research Question

The central research question guiding the study was: what strategies do business managers in United States DoD contracting companies use to fill cybersecurity positions? The focus of the research was to find business managers with successful hiring practices for hiring cybersecurity professionals for DoD cybersecurity contracts. I collected data from face-to-face interviews and a review of current job postings for the organizations of the participants.

Interview Questions

The interview questions were:

1. How did you find skilled/qualified cybersecurity professionals?
2. How similar is the training potential new hires receive to what your organization requires?
3. What are the strengths in your hiring process?
4. What are the weaknesses in your hiring process?
5. What training opportunities does your organization offer to prepare future cybersecurity professionals?
6. What levels of education and or training do you think cybersecurity professionals need to become efficient in your organization?
7. What are the threats to your organization when cybersecurity professionals in your organization do not have the required training?
8. How does your organization ensure the cybersecurity staff has the necessary training?
9. What training method produces cybersecurity professionals you would hire certification, education or both and why?
10. What additional information can you provide to assist me in understanding the phenomenon?

Conceptual Framework

The conceptual framework used for this study was the organizational learning theory. Chris Argyris and Donald Schon developed the organizational learning theory in

1974. Argyris (1976c) explained concepts such as *single-loop* and *double-loop learning*. Learning occurs when the organization's leaders identify for the first time the intersection of the intent of a process and the results of the process (Argyris, 1996). The leaders and operators learn process efficiency by detecting and correcting deficiencies in the process (Argyris, 1996). Single loop learning is a learning style that reacts to a precondition (Argyris, 1976c). Single loop learners cannot make decisions about the changing conditions (Argyris, 1976c). Double loop learners have the ability reevaluate the situation and change the process as necessary (Argyris, 1976c).

The organizational learning theory applied to the study because the theory explains a method that companies can use in recruiting, hiring, training, and maintaining the organization's cybersecurity team. Organizations that use organizational learning increase innovation and the performance of the organization (Jiménez-Jiménez & Sanz-Valle, 2011). Implementing the organizational learning theory is a technique to develop a foundation for building processes and developing a culture of continuous learning in the cybersecurity hiring process.

Operational Definitions

The following are the unique terms used in this study:

Collective knowledge. Collective knowledge is the process of accumulation and dissemination of rules and procedures in an organization used for problem solving and process improvement (Hecker, 2012).

Cybersecurity. Cybersecurity is a term used to describe all aspects of information security involved in protecting, monitoring, and maintaining systems and data (Von Solms & Van Niekerk, 2013).

Department of Defense (DoD) contracting. DoD contracting is a method of completing tasks for the DoD by hiring outside organizations. The U.S. Congress authorizes the DoD to enter into the contract. The contract obligates the DoD and the U.S. government to provide money in return for the contracting company's provision of a service or product (Schwartz, Ginsberg, & Sargent, 2015).

Organizational learning. Organizational learning involves gathering information, analyzing the information, and using the outcome of the analysis to enhance the organization's ability to execute a business function (Pokharel & Choi, 2015).

Risk management. Risk management is the continuous process of identifying assets, identifying threats to assets, and implementing mitigation strategies to protect assets (Dawson Jr., Crespo, & Brewster, 2013).

Assumptions, Limitations, and Delimitations

Assumptions

An assumption in research, as defined by Leedy and Omrod, (2013), is a self-evident truth about the topic that the researcher believes is true without concrete evidence. The assumption must be a true statement, or the assumption is meaningless to the research (Leedy & Omrod, 2013). The first assumption that I had in this study was that business managers use a systematic method for hiring new cybersecurity professionals. The second assumption was that the method and the design that I chose for the study were the most suitable method and design. The third assumption was that DoD organizations requesting cybersecurity services from contracting companies are acccurately describing the contractual services needed to complete the organizations mission. My last assumption was that the population targeted for participants would have enough volunteers to reach data saturation.

Limitations

Limitations are weaknesses in any part of the research (Leedy & Omrod, 2013). A limitation of this study was the exclusion of information from cybersecurity professionals in other regions of the world. The study includes only DoD cybersecurity contractors in the United States, specifically Hampton Roads, Virginia. Not including other regions was a weakness because cybersecurity professionals in other countries may face a different set of threats (S. Kim, Wang, & Ullrich, 2012). The different threats may require the other country's cyber workforce to use tactics, techniques, and procedures to address these issues that are not used by the cyber workforce in the United States. The way other countries view and implement learning may be different based on the unique experiences of the respective cyber workforce. The final limitation was the lack of generalization of the results of the study to other agencies or other industries.

Delimitations

Leedy and Omrod (2013) defined delimitations as the boundaries of research. The intent of the study was to gain information from cybersecurity professionals in Hampton Roads, Virginia. Men and women in the information security segment of IT were the focus of the study. Other facets of IT, such as database administration or web application development were not the focus of data collection.

Significance of the Study

Contribution to Business Practice

This study contributes to business practice by exploring the methods used by business managers when filling cybersecurity positions. Cybersecurity is a profession with highly trained professionals who implement the security measures required to protect an organization's information systems (Hoffman, Burley, & Toregas, 2012). Hiring cybersecurity professionals requires additional investment in their training (Suby & Dickson, 2015). Ensuring that cybersecurity employees receive the training needed to remain relevant in the field adds value to the employee, which in turn, adds value to the organization. The value created in the relationship translates into an organization with the right personnel and motivation to provide excellent service to the organization's customers (Strohmeier, 2013).

This study may give business managers a broader understanding of the requirements of hiring cybersecurity professionals to provide the desired protection of information systems and data. The study may also provide human resource (HR) leaders with an understanding of the differences in the qualifications the organization requires to successfully hire cybersecurity positions for DoD contracts.

Implications for Social Change

The results of the study may support positive social change by providing business managers in the U.S. DoD contracting industry with strategies for filling cybersecurity positions. The study will give colleges and universities a glimpse at the results of the cybersecurity professionals hiring practices, which can give students looking for cybersecurity careers an understanding of what to expect when applying for cybersecurity positions on DoD contracts. The concept of cybersecurity is relatively new, and there is a lack of scholarly knowledge on the topic. This study may contribute to the body of literature in cybersecurity results and strategies to help fill cybersecurity vacancies, and to provide future researchers a starting point for further research on the topic.

A Review of the Professional and Academic Literature

The purpose of this qualitative case study was to explore the strategies that business managers in U.S. DoD contracting companies use to fill cybersecurity positions.

The literature review for the study comprises scholarly articles regarding cybersecurity and organizational learning. The following topics appear in the literature review: *organizational learning, cybersecurity, perceptions cybersecurity training, information systems risk, information systems security frameworks,* and *the cyber impact*. The review of the topics should give the reader a solid understanding of what cybersecurity is, the existing training, the risks information systems encounter, the frameworks used to secure systems, and the overall impact of cybersecurity on organizations.

The most effective method used to review the literature on the subject was to conduct a keyword search using Google Scholar. The keywords used were *organizational learning, learning organizations, cybersecurity, information assurance, cyber training,* and *cyber certifications*. I configured Google Scholar to connect to Walden University's library to ensure that the articles in the database would be available.

There are 116 sources in this study. One hundred and one sources are 5 years old or less, and 101 of the 116 sources are peer reviewed. There are 79 sources in the literature review, and 74 of the 79 sources are peer-reviewed. The percentage of peer-reviewed sources is 86%. The percentage of sources 5 years old or less is 87%. The percentage of peer-reviewed sources in the literature review is 93%.

Organizational Learning Theory

The literature on organizational learning provides the details and background of the theory. The major themes discussed are single-loop learning, double-loop-learning, and negative and positive benefits of applying the theory to an organization. The terms learning organizations and organizational learning are interchangeable terms throughout the literature (Pokharel & Choi, 2015).

Organizational learning involves gathering information, analyzing the information, and using the outcome of the analysis to enhance an organization's ability to execute a business function (Pokharel & Choi, 2015). Jimenez-Jimenez and Sanz-Valle (2011) conducted research showing organizational learning, innovation, and organizational performance have a positive relationship with each other. Goh, Elliott, and Quon (2012) also found a significant positive relationship between learning and performance. Jiménez-Jiménez and Sanz-Valle (2011) suggested that organizations using the organizational learning strategy have a positive correlation between innovation and increase their overall productivity.

Pillars of organizational learning theory. Single-loop learning and double-loop learning are two essential tenets of organizational learning. Single-loop learning appears when a process changes because of a known deficiency (Argyris, 1996). A simplified example of single-loop learning is a checklist. There is no deviation from the checklist, and the result should be the same every time an employee completes the checklist. If the individual or system requires a change, the individual must change the entire process to complete the task. The goal of the individual in single-loop learning is to adhere to the governing values which are winning, hiding negative feelings, and adhering to the rational of the process to achieve the desired purpose (Argyris, 1976a). The problem with using the single-loop learning is that the method does not provide the proper feedback needed to enhance the efficiency of the process. Individuals will only do as instructed in the process to prevent singling themselves out in the organization (Argyris, 1976b).

Double-loop learning occurs by changing the fundamental principles of the processes, and subsequently, the actions in the process change (Argyris, 1996). When using double-loop learning, the individual or group can reexamine the task to add efficiency to the process. Double-loop learning provides the opposite effect of single-loop learning. The two learning strategies require adherence to the same governing values, but double-loop learning also requires valid information, commitment and free, informed choice for the individual (Argyris, 1976a). Free and informed choice, valid information, and commitment give the individual the authority to articulate personal views and to add input into the process without fear of reprisal from senior management. The result of double-loop learning is an increase in the effectiveness of decision-making and an increase in the effectiveness of the monitoring of decisions by management. The implementation of double-loop learning also increases communication between management and induvial employees tasked with correcting errors in a process (Argyris, 1976a).

The competitive advantage of learning. Organizational learning is the process of gathering information, distributing information, interpreting information, integrating information, capturing information, and then institutionalizing the information (Flores, Zheng, Rau, & Thomas, 2012). The goal of organizational learning is to adapt to the changing environment by developing new processes (Flores et al., 2012). Maintaining the ability to adapt allows the organization to gain a competitive advantage because the processes allow the organization to apply institution knowledge to emerging business problems (Lengnick-Hall & Inocencio-Gray, 2013).

The process starts with employee knowledge, skills, and attributes necessary to complete the assigned tasks (Caldwell, 2012). Once the employee obtains the knowledge, skills and attributes, the individual has the requisite knowledge to shift the paradigm from an individual view to an organizational view (Caldwell, 2012). The organization must have a clearly defined vision (Pokharel & Choi, 2015). Organizations operating under a defined vision empower employees to provide more input because the employer may value their opinion (Alt, Díez-de-Castro, & Lloréns-Montes, 2014). The senior leadership of the organization produces the vision, but the implementation is the responsibility of the employees. Participating in the vision gives the employees a sense of ownership. The result of exercising the vision prepares the organization for organization-wide learning

(Pokharel & Choi, 2015).

Rival theories. Two theories found in the current literature rivaling the organizational learning theory are the dynamic theory of organizational knowledge creation and the theory of the firm. The dynamic theory of organizational knowledge creation posits that organizations create and expand knowledge through four patterns of interaction: socialization, combination, internalization, and externalization (Nonaka, 1994). There is no alignment between the dynamic theory of organizational knowledge and the intent of the study because the problem is not about how organizations create knowledge, but the implementation of created knowledge. The theory of the firm is a theory used to describe and anticipate the structure and behavior of an organization. The theory is not a single theory, but a multitude of theories used to explain an existing phenomenon in different organizations (Grant, 1996). There is no alignment between the theory of the firm and the intent of this study because the problem does not involve the structure and behaviors of the organization.

Cybersecurity

The literature on cybersecurity is a collection of articles about the current state of cybersecurity and some aspects organizations must consider when building a cybersecurity program. There is a shortage of cybersecurity professionals in all industries in the United States (Suby & Dickson, 2015). The cybersecurity field emerged because of a need to protect data and systems from unauthorized access and to ensure the availability of data to the data owner (Dunn Cavelty, 2014). The definition of cybersecurity is the protection of information from threats while allowing an organization to operate in an environment with lower risks to information systems (von Solms & van Niekerk, 2013). Cybersecurity and information security are terms used interchangeably to describe all aspects of information security by protecting, monitoring, and maintaining systems and data (Von Solms & Van Niekerk, 2013).

One mechanism used by organizations to develop a strong security posture is a security policy (Ifinedo, 2014). Each organization writes the policy to align with the assets of the organization. No two networks operate for the same purpose or provide the same functions for the supported organization (Nielsen, 2012). Creating nonaligned security policies may leave gaps in the organization's security posture. The exposure can lead to data loss or damage if attackers exploit the security gap (Dunn Cavelty, 2014). The presence of a strong security policy, enforced across the organization, is the starting point for a secure computing environment.

The U.S. government recognizes the cybersecurity problem and began the implementation of a robust cybersecurity plan for the country's government, but the cybersecurity plan does not include private organizations in the United States (Nielsen, 2012). Private companies constantly underfund the their cyber protection (Sales, 2013). Corporate governance must align information systems with business goals and objectives (Jirasek, 2012). When all the factors are in place, the organization has a better chance against attackers when attempting to protect the confidentiality, integrity, and availability of the organization's data and systems.

Private companies accept the risk of not implementing strong cybersecurity policies, even though the number of cyber crimes increased against private organizations nationally (Hiller & Russell, 2013). Private organizations did not have the correct incentives to motivate the leaders of the organization (Maughan, Balenson, Lindqvist, & Tudor, 2013). The overwhelming attitude of the private sector is that cybersecurity is important, but private sector organizations do not know how much cybersecurity their organization requires (Huang & Behara, 2013).

The U.S. military uses the Cyber Command to protect its military networks while the Department of Homeland Security protects all other government agencies (Eztioni, 2011; Nielsen, 2012). The need for profit is a consideration for private companies when implementing security measures (Huang & Behara, 2013). Private companies want the government to invest in technologies to ensure that the private companies can use the new technology in the future. In 2011, President Obama introduced a security plan to help integrate the private sector into the government protected security infrastructure. The National Initiative for Cybersecurity Education (NICE) developed an awareness program intended to raise the cyber knowledge of the everyday user (Furman, Theofanos, Choong, & Stanton, 2012). NICE also has a national data breach reporting policy, which motivates private companies to implement standard level of security to ensure they need not disclose a data security breach to the public (Eztioni, 2011).

An emerging area of interest in the current literature is the cyber criminal. Many characteristics of ordinary criminals exist in the criminal profile of cyber criminals (Warikoo, 2014). The major difference is that the cybercriminal has the ability to use technology as an offensive weapon. The research described three types of cyber criminals. The first is the idealist. The major motivation for this type is to gain social recognition. The attackers in the idealist category rely on automated attacks (Potts, 2012). The attacks are programs or scripts executed by attackers. Idealists use open source tactics, techniques, and software that are easy to detect with antivirus software (Potts, 2012).

The next cybercriminal is sophisticated and motivated by personal greed. A major difference in the classifications of cybercriminals is the methods cybercriminals during an attack (Hoque, Bhuyan, Baishya, Bhattacharyya, & Kalita, 2014). Instead of using the tools to find vulnerabilities to help the organization, the criminals use their skills and knowledge to profit based on their ability to attack an organization's users and information systems. Cyber criminals buy the tools on the black market and use the tools to steal information—such as credit card numbers—with the intent of selling the credit card numbers for financial gain (Potts, 2012).

The final cyber criminal is the cyber terrorists. Cyber Terrorist use cyber-criminal activities to terrorize people and countries (Hua & Bapna, 2013; Moslemzadeh Tehrani, Abdul Manap, & Taji, 2013). One of the questions raised in the literature is how do countries police cyber terrorism when the actives cross international borders (Hiller & Russell, 2013; Moslemzadeh Tehrani et al., 2013; Nielsen, 2012; Rid & Buchanan, 2014). Attributing cyber-attacks to a specific attacker is difficult for both governments and private organizations (Rid & Buchanan, 2014). Quigley, Burns, and Stallard (2015) suggested governments and private organizations must have a real understanding the cyber posture and the true nature of the vulnerabilities to develop a strategy to stop cybersecurity terrorists.

Potts (2012) also included two more categories, which are advanced persistent threats and insider attacks. Insider attacks initiate from physical access to network and information systems assets. Authorized insiders access systems and the information stored in the organization's information systems (Posey, Roberts, & Lowry, 2013; Willison & Warkentin, 2013). Attacks from insiders range from accidental or incorrect data entry to intentionally malicious activity by the insider (Willison & Warkentin, 2013). Tactics such as social engineering allow attackers to gain access to the network and infect the information systems or steal important company information (Cokley & Awad, 2013). The advanced persistent threat (APT) is the biggest threat and can cause the most damage to an organization (Potts, 2012). Advanced Persistent Threats are sophisticated attackers using methodical attack processes to gain and maintain system access (Potts, 2012). The attacks used by APTs target the people using computers and not the computer (Julisch, 2013). The reason for attacking people first is to gain confidential, proprietary, or classified information from the targets. The process of targeting and attacking can take years (Potts, 2012). Using information systems is the norm in countries with the infrastructure to support networked communications. Implementing security measures to protect against attackers is a task all users share. The level of understanding necessary to combat criminals, while reducing costs is a goal of all users (Garfinkel, 2012).

Another part of cybersecurity is the disclosure of vulnerabilities after discovery. Ransbotham and Ramsey (2012) conducted a study examining the disclosure of vulnerabilities and asks the question; are the markets for vulnerability disclosure effective? Two actors may find vulnerabilities in information systems: attackers and security professionals. The disclosure path for the attacker moves from discovery to the black market. The attackers find the vulnerability and sell the vulnerability and or use the vulnerability to exploit systems (Ransbotham & Ramsey, 2012). While vendors preferred full disclosure, Bergman (2015) posited requiring disclosure of any kind is a violation of the first amendment to the U.S. Constitution.

Cybersecurity professionals choose one of three initial paths: Immediate disclosure, non-public disclosure, and market disclosure (Ransbotham & Ramsey, 2012). The cybersecurity professional may release the information publicly without informing any agency beforehand. Releasing the information first is dangerous because the information could lead to the development of exploitation code by an attacker (Bergman, 2015). The researcher has the option of a non-public disclosure. A non-public disclosure gives the vendor and interested parties a chance to develop a countermeasure before the vulnerability or exploit code reaches the public. The final way to disclose vulnerabilities is market disclosure. Market disclosure means people or organizations with a subscription to the vulnerability market receive information from the security researcher about the exploit. The security researcher gives the subscriber information to help protect the organization's information systems from the exploit. The vendor receives the exploit with the expectation the vendor will fix the problem (Ransbotham & Ramsey, 2012).

Senior management creates the security culture of an organization (Kwon, Ulmer, & Wang, 2012). The Chief Information Security Officer (CISO) is often the catalyst for the security culture (Kwon et al., 2012). The CISO is a person with knowledge and experience in both information technology and information security. The CISO creates security policies and enforces the policies throughout the organization (Kwon et. al., 2012). The CISO must know both business functions and information security functions. The CISO is the translator for the other senior-level executives in the organization. The policies at the senior level produce administrative controls for the organization. There are also technical controls, implemented using technical techniques and used to prevent unwanted activity (Lowry, Posey, Roberts, & Bennett, 2014).

Other research examined specific devices used for cybersecurity. Pachghare (2012) examined the use of intrusion detection systems (IDS) and the importance of fine-tuning the IDS to detect attacks. Zarrabi and Zarrabi (2012) discussed using cloud-based IDS instead of the traditional inline IDS found in many networks today. The concept is the organization deploys a client on the systems which reports to an IDS service in the cloud. The IDS will do the analysis of the traffic to determine if the traffic is malicious (Zarrabi & Zarrabi, 2012). An IDS can be an effective form of perimeter defense, but security does not stop at the perimeter (Dawson Jr. et al., 2013). Cybersecurity professionals must consider how to implement security at the system level.

An example of an information system needing protection is the human resources information management system. Human Resources Management Systems (HRMS) store and retrieve the human resources related data for an organization, connect the organization to customers and provides a collaboration to for business segments (Strohmeier, 2013). The information in the system makes the HRMS one of the most critical information systems in an organization (Zafar, 2013). A human resources system is a complicated system with several technologies requiring consideration when developing a security strategy. The system has databases, user interfaces for the application, and hardware requiring security. Changing one or more configurations on one specific system could leave the organization’s vulnerabilities exposed. Each of the technologies has specific vulnerabilities which require specific security considerations (Zafar, 2013).

Of all the tactics, techniques, and procedures discussed in the literature, the most critical and the most vulnerable part of cybersecurity is the user (Green, 2015). The lack of proper security training of users and inadequate security measures make the user the easiest target to exploit (Jenkins, Grimes, Proudfoot, & Lowry, 2013). Determining the best way to deliver training depends on the users in the organization (Abawajy, 2014). Determining how to deal with security policy violations by users in the organization is one of the areas of discussion.

Chen, Ramamurthy, and Wen (2012) discussed three techniques for user punishment, coercive, remunerative and normative punishment. Punishment for security violations influences behavior when the punishment is clearly defined (Cheng, Li, Li, Holm, & Zhai, 2013). Cox (2012) used a different approach to dealing with users. His research builds upon the theory of planned behavior. Cox suggested attitudes toward behavior, subject norms, and perceived behavior beliefs are the major constructs in why humans commit certain actions. The biggest influence occurs when senior management participates in the security process (Hu, Dinev, Hart, & Cooke, 2012). Employees comply with security policies when senior management clearly explains how security fits into the overall strategic goals of the organization. If the organization’s strategic goals do not align well with the overall cybersecurity efforts, then the employees will complain based on the participation of the senior leadership (Hu et al., 2012).

The current literature on cybersecurity offers a wide range of subjects to consider. Policy, technology, leadership, and users all have a role. In some cases, one role sets the stage for the other, but all are important, and all are necessary. Cybersecurity is a growing segment of IT (Suby & Dickson, 2015). The level of cybersecurity increases when organizations implement a strong security policy (Ifinedo, 2014). Cybersecurity is important to both government organizations and private companies; however, the key to effective implementation is to align information systems with business goals and objectives (Jirasek, 2012).

Perceptions of Cybersecurity Training

The overall theme discovered in the literature on cybersecurity training is the shortage of trained cyber professionals. There is no consensus in the literature on the most effective way to train the cyber workforce. The current cybersecurity workforce does not have the training or resources to handle the daily challenges in cyberspace (Hoffman et al., 2012). Addressing the lack of training and resources is a high priority for organizations globally (Hoffman et al., 2012). A cybersecurity professional has to understand all areas of IT (Burley, Eisenberg, & Goodman, 2014). Developing an understanding in all areas of IT takes years of training and hands-on experience to develop the proficiency needed for success. The skills required for each position have substantial differences which may hinder cyber professionals from mastering security at all levels (Hoffman et al., 2012). Cybersecurity professionals start with the entry-level certifications such as CompTIA's Security + and work towards advanced certifications such as ISC^2's Certified Information Systems Security Professional (CISSP) and ISACA's Certified Information Security Manager (CISM). The CISSP requires the candidate to pass a 225-question test as well as prove 5 years of experience in two of the ten knowledge domains of the test. After the candidate passes the test, the candidate must gain the endorsement of a CISSP in good standing with the organization (ISC, 2016). The CISSP is one of the top certifications, but not every cyber position requires the CISSP certification. There are several sub-disciplines within cybersecurity requiring cybersecurity professionals to learn enough about each area to provide the necessary protections for the organization's information systems (McGettrick, 2013). The method of cybersecurity training for cybersecurity professionals depends on the type of training program, but the goal is to have a uniform set of training objectives across the cybersecurity spectrum (McGettrick, 2013). H. Chen et al. (2012) described a program of instruction used to develop engineers in China. The intent of the program is to have a standardized training process for all computer engineers. The training process gives the engineer an understanding of professional ethics, specialized knowledge, and technology project management and communication skills. The expectation of any graduate of the program is to have the above qualities along with the ability to solve critical computer engineering problems (Chen et al., 2012). The plan for growth presented as a training program by Chen et al. (2012) is to focus on the youth of the country and not just the certification of an aging cybersecurity workforce.

There is a scarcity of scholarly literature on the subject of cybersecurity training. The few articles found about the subject offer innovative ways to tackle the problem. Kostakos (2012) told the story of the methods used to train members of the military. The method of training military occupations gave insight into how to transform IT and computer science training in colleges and universities. Kostakos’ training consisted individual tasks and group tasks. Individuals learned how to complete the tasks individually and as a team. The concept is true for cybersecurity training, as well. There are tasks each security professional must know and understand while the larger, more abstract security challenges require participation from employees in the IT department, as well as participation from employees of other departments in the organization (Podhorec, 2012). The current training curricula lack standardized training of the tasks necessary to effective cybersecurity implementation (Paulsen, Mcduffie, Newhouse, & Toth, 2012)

To make the concept work, proficiency benchmarks for cybersecurity are required. Cranor and Sadeh (2013) added to the discussion by exploring the aspect of training for privacy engineers. Privacy is an integral part of all disciplines of information systems security (Hiller & Russell, 2013). The solution to closing the gap is to begin adding privacy training as part of undergraduate and graduate programs. Adding the programs might introduce computer science students to the idea of implementing the concepts of privacy throughout the entire software development lifecycle. Some institutions such as Carnegie Mellon have already started implementing privacy training, but the training has not spread across academia (Cranor & Sadeh, 2013). The same is true in the focal area of cryptography (Mcdonald & Andel, 2012).

The theories in information systems security, such as cryptography and access control, are easy to teach but hard to demonstrate and harder to master. Teaching the concepts may take more time than the professors have per semester. The key to giving the students the experience needed is to add the hands-on component to the curricula (McGettrick, 2013). Cybersecurity challenges such as capture the flag helps the student develop the security mindset (Gavas, Memon, & Britton, 2012). The cybersecurity competition gives the student a chance to practice both the offensive and defensive side of cybersecurity. The competition allows the student to understand the amount of effort and knowledge required to develop security solutions against an active cyber aggressor (Bei, Kesterson, Gwinnup, & Taylor, 2011). The use of cyber competition teams allows the students to see the theory learned in class.

Once the cybersecurity student has moved from a school environment to the work environment, specific job-related training is necessary to hone skills and to evolve as technological advances continue to progress (Conrad, 2012). Kebbel-Wyen (2012) documented a case study of Adobe's ability to transform the organization from one of the worst in security to among the best. Adobe created the Asset Certification Program (ACP) to produce high quality, security-minded software engineers (Kebbel-Wyen, 2012). In 2008, before the creation of the ACP program, Adobe's average response time of zero-day attacks was 57 days. By 2012, Adobe reduced the response time of zero-day attacks to 10 days (Kebbel-Wyen, 2012).

Of all the requirements for cybersecurity, one area requiring emphasis is the ethics of the profession; however, there is a lack of scholarly literature about ethics in cybersecurity. Most professions adhere to a code of ethics, which guides the industry: cybersecurity should not be any different (Dunn Cavelty, 2014). In fact, there may be a superlative need for cybersecurity professionals to uphold a higher level of ethics because of the type of data maintained. For example, cybersecurity professionals in a hospital protect sensitive patient information, as well as sensitive employee information. The purposeful compromise of information could potentially ruin the lives of the employees and patients as well as leave the organization vulnerable to government penalties and lawsuits (Green, 2015). Posey, Roberts, and Lowry (2013) suggested learning, practicing, and implementing ethics into cybersecurity training may help to deter otherwise honest people from unethical actions as cybersecurity professionals.

The literature related to perceptions in cybersecurity training focuses on growing cybersecurity workforce, the lack of a strong cybersecurity educational pipeline, and the need for ethics in the profession. Training is an essential element for all professions. As in other professions, cybersecurity professionals need the requisite training in the field to become masters of the craft (Hoffman et al., 2012). Training is both an organizational responsibility and a personal responsibility. Collective tasks and personal task mastery are an integral part of the training process (Podhorec, 2012). Personal mastery is the applicable element of the organizational learning theory for the section. Personal mastery is one of the steps necessary to begin the organizational learning process (Jiménez-Jiménez & Sanz-Valle, 2011).

Information Systems Security Risk

The major topics in the literature are risk management and implementing risk management. Dawson Jr., Crespo, and Brewster (2013) defined security risk assessment as a continuous process for examining the security posture and risks of the system and identifying countermeasures for the risks. The first step is to identify the organization's assets. The second step is to conduct a vulnerability analysis. Vulnerability analysis includes developing or choosing a risk management methodology, identifying and analyzing the risk, and determining the best method to mitigate the identified risks (Dawson Jr. et al., 2013). The process identifies vulnerabilities and determines appropriate mitigations to provide both security and functionality. Patch management is one of the common mitigations for vulnerabilities (Maisey, 2014). The process of implementing patches should include considerations for loss productivity due to system downtime and the possibility of rendering the system or programs on the system inoperative (Ioannidis, Pym, & Williams, 2012).

An important factor to consider when choosing a way to manage information systems security risk is how the implementation of the countermeasures affects the ability of the organization to meet its business objectives. Organizations use information technology to achieve business objectives (Abawajy, 2014). Jirasek (2012) showed the relationship between information security and business security strategies. Information security is not a separate function, but a subset of the strategic business security strategy for the organization (Jirasek, 2012). Security managers must define the security objectives for the organization. Each security objective must support a business objective

(Jirasek, 2012). Once defined, the implementation of the administrative and technical security control measures follows. Administrative controls are controls implemented through policies. Some of the controls include risk assessments, media protections, configuration management and contingency planning (H. B. Kim, Lee, & Ham, 2013). Technical controls are the controls placed on the information system allowing or denying a user to perform certain tasks (Lo & Chen, 2012). After identification and implementation of the controls, business processes aligned with the controls. The overall objective is to balance security and functionality (Jirasek, 2012).

The tenets of organizational learning exist in the information systems security risk management process. Despite the connection, there is no current literature presenting an argument for organizational learning in the information systems security risk process. The literature on information systems security risk implementation is about different techniques used to implement information systems security risk management, the benefits of information system security risk implementation, the potential issues implementation could cause, and the process for information systems security risk assessments (Dawson Jr. et al., 2013; Ioannidis et al., 2012; Jirasek, 2012; Lo & Chen, 2012). The preceding section describes what information systems security risk is. The next section provides an explanation of how to implement the process.

Information Systems Security Frameworks

Information systems security frameworks literature is a review of the major security frameworks used by governments and by private businesses. Security frameworks are building blocks for a secure network (Scully, 2011). Frameworks also provide an opportunity for learning to flourish. The type of framework used may apply to organizations such as the defense information assurance accreditation and certification process (DIACAP) used in the DoD (Dawson Jr. et al., 2013). Other organizations have the freedom to use any framework available to the organization. Cybersecurity professionals must have the knowledge and skills to tailor the framework to fit the specific situation (Paulsen et al., 2012). The popularity of studying and creating security frameworks is evident by the number of scholarly articles exploring the effectiveness of the various frameworks. In the majority of the articles, the framework is the bulk of the discussion; however, the underlying issue discussed is the implementation of risk management for information systems.

Several organizations produce security framework standards. The International Organization of Standardization (ISO) and the National Institute of Standards (NIST) are the biggest contributors to the development of security frameworks (Clinton, 2015). The ISO produces a set of documents known as the Information Security Management Systems (ISMS) standards. The documents included are ISO 27000, ISO 27001, ISO 27002, and ISO 27005 (Faris, Medromi, Hasnaoui, Iguer, & Sayouti, 2014). The ISO standards, specifically the ISO 27000 certification, show the organization has the ability manage information systems effectively and efficiently. The ISO 27000 certification also shows the organization has documented and repeatable processes in place. ISO 27000 is a detailed standard and gives the security professional a better understanding of how to complete certain tasks associated with applying the framework. The disadvantage is the framework does not integrate with other security frameworks the organization (Faris et al., 2014).

Two security frameworks can coexist after major adjustments to each framework. NIST produces a series of standards known as the SP 800 series. The standards started in 1990, and to date, the set of standards are the most comprehensive set of standards on the market for information systems security (Clinton, 2015). The DOD uses a process called the DIACAP as a security framework (Dawson et al., 2013). The U.S. Navy uses a team-centric approach to accomplish information assurance goals (Dawson et al., 2013). The DIACAP identifies information assurance responsibilities by position. Categories group information assurance controls and consider all areas of security. Organizations will apply the controls necessary to obtain the level of security dictated by the mission assurance category level. Each level of mission assurance has different requirements to satisfy each control. Mission assurance category one is the most restrictive while mission assurance category three is the most permissive (Dawson Jr. et al., 2013).

Another organization developing security frameworks is the Information Systems Audit and Control Association (ISACA). The main framework is the Control Objective for Information Related Technologies (COBIT). The advantages of using COBIT are the alignment of business practices and IT, the flexibility of by allowing best practices to implement, and fosters a fluid information systems environment where changes may support business objectives (Whitman & Mattord, 2012). The disadvantage is the type of attacks organizations face today are dynamic, consisting of customized attacks developed to bypass standard technical controls (Baskerville, Spagnoletti, & Kim, 2014). Cyber professionals have to design security measures creative enough to meet the standard as well as outsmart the attackers. The literature is about the information systems security frameworks currently used in cybersecurity. The frameworks are learning processes developed to protect information systems (Scully, 2011). Cybersecurity professionals leveraging the frameworks possess the ability to implement learning in the cybersecurity processes

In the majority of the articles, the framework is the bulk of the discussion; however, the underlying issue discussed is the implementation of risk management for information systems. The major frameworks used by private companies are NIST (Faris, Medromi, Hasnaoui, Iguer, & Sayouti, 2014) security frameworks and COBIT by ISACA (Whitman & Mattord, 2012). Government organizations use a specific security framework called DIACAP (Dawson et al., 2013). The implementation of any security framework will increase the organization's ability to detect and react to attacks (Scully, 2011).

Cyber Impact

The major focus is the negative impact improper cybersecurity management has on organizations. The increased need to protect information systems and data spawned the highlights the importance of information assurance (Lai, 2012). The goal of information assurance is to protect the availability, confidentiality and the integrity of information systems and the data stored on the systems (Drtil, 2013; Kumar & Singh, 2012). Drtil (2013) discussed how information security works in theory and how cybersecurity works in reality. The areas discussed are the concepts of confidentiality, integrity, and availability.

Using information systems to accomplish detailed specialized tasks, or everyday tasks do not come without risk to the data and the information systems. Kim, Wang, and Ullrich (2012) conducted a study of reported cyber-attacks of various governments and nations. S. Kim et al., (2012) suggested the lack of coordination and collaboration among the primary stakeholders hinder the effort to combat cyber crime. There is a lack of data sharing and coordination between governments and private companies (Quigley et al., 2015). The lack of coordination allows cyber crimes and criminals to go undetected and unpunished for the havoc unleashed on the world's information systems. S. Kim et al. (2012) also posited the attackers receive better training than the defenders and the investigators. An international treaty would forge a bond and define common objectives for participating countries (S. Kim et al., 2012).

Deciding which target to attack has an economic as well as a strategic element. Some of the common attacks used in the current landscape are phishing, pharming, and man in the middle attacks (Huang & Behara, 2013). The attacker must choose which approach will work for the situation. Herley (2013) described an economic approach to choosing targets for cyber-attacks. Herley described two basic types of attacks: scalable and non-scalable. Scalable attacks are attacks where the number of attacks does not raise the cost to attack. The attacker uses the type of attack, which fits the intent of the attack.

A computer network attack is an act of destruction, denial, the degradation, or destruction of a system or network (Herley, 2013). Computer network exploitation is an intelligence gathering activity (Rustici, 2011). The definition used for the computer network attack is kinetic, meaning the definitions used to describe the attack mirror definitions used to describe how military hardware, such as tanks, operate. Cybersecurity is a weapon similar to air power, sea power and land power in the traditional three-dimensional battle space (Rustici, 2011). Phishing and drive-by websites are ways attackers use cyber assets to attack the target (Herley, 2013). While there are costs associated the activities, the cost per attack is low. Non-scalable attacks have a linear cost dependence on the number of users attacked. If the attacker doubles the number of attacks, then the cost of the attacks also doubles. An example of a non-scalable attack is a social engineering attack (Herley, 2013).

Physical security attacks are another example of non-scalable attacks. The cost to attack using physical attacks and social engineering attacks increase with the number of potential victims. The attack technique used depends on the purpose of the attack. A strategic cyber-attack can be more disruptive than dropping several one thousand ton bombs on a country. Especially in the United States, which depends heavily on network systems for daily operations (Rustici, 2011). If the intent is to obtain a million dollars from a person, then the attacker may use precision, non-scalable attack. If the intent of the attack is to defraud any person with no specific idea of how much he or she will make per transaction, then a scalable attack will work the best (Herley, 2013).

Cyber-attacks affect the way organizations plan and implement information systems. A study conducted by Das (2012) posited information systems data breaches rose from 18% in 2009 to 27.3% in 2010. The highest number of reported incidences came from banking, financial services, insurance companies, and e-commerce companies. E-commerce based business had an average loss of $30 million in revenue, which also included the loss of productivity of employees. Attacks against organizations such as banks and insurance companies have an impact on the stock prices for those companies. Gordon et al. (2011) conducted an examination of current literature on stock prices and security breaches and found that there is a statistical significance between information systems breaches and the stock market value of the breached companies.

There are nearly two billion Internet users around the world (Scully, 2011). Each day, there is an average of 294 billion e-mails and five billion text messages sent by the users (Scully, 2011). The majority connect to the Internet via computers. Businesses adapt to change by using the technology; however, businesses introduce new risks in the form of cyber threat (Scully, 2011). Scully used a diagram to display the cyber threat spectrum. The cyber threat spectrum is in the shape of a triangle. At the apex, the script is kiddie (Scully, 2011). A script kiddie is a beginner and has limited scope and limited abilities. At the base of the triangle, is the state-sponsored cyber threat. State-sponsored hackers are well-trained, highly technical, highly sophisticated hackers with support from a government agency (Scully, 2011). State-sponsored hackers and industrial spies focus on targeted attacks (Lai, 2012). State-sponsored hackers look for vulnerabilities in social and technical aspects of the organization (Scully, 2011).

Penetration testers help organizations find vulnerabilities in the organization’s networks in the same manner used by state-sponsored attackers use (Conrad, 2012; Scully, 2011). Even with the legal and ethical constraints, penetration testers succeed because organizations tend to protect the outside while the inside of the network is vulnerable. The advanced persistent threat exploits targeting networks for information. Penetration testers have the technical ability and resources to wage full-scale cyber warfare against the targets. A full-scale attack includes physical penetration, social engineering, and network penetration (Maisey, 2014). One of the many problems discussed is the lack of communication between senior leadership and security. The security team may identify and rectify problems from cyber threats without the senior management knowing the situation happen. One way to minimize the risk and to keep management informed is to implement a security framework. The framework should include threat analysis, capabilities assessment, continuity of operations plans, detection capabilities, and data segregation, in a recovery plan (Scully, 2011). The literature is about the impact cybersecurity has on an organization.

Literature regarding ways to protect data and literature detailing the type of cyber threats exists; however, I found a gap in the current literature concerning the potential benefits of using a learning process to protect data. The major focus is the negative impact improper cybersecurity management has on organizations. A lack of coordination and collaboration among the primary stakeholders in organizations hinder the effort to combat cybercrime (S. Kim et al., 2012). The decision to target a system has an economic impact on the attacker. The attacker compares the cost of the attack to the potential impact of the attack when making the decision about which organizations to attack (Huang & Behara, 2013). Once the attacker has determined the target, the attacker develops the attack vector. The attack vector depends on the goals and objectives of the attack (Rustici, 2011). Organizations prepare their information systems by applying a security framework, which includes threat analysis, capabilities assessment, continuity of operations plans, detection capabilities, and data segregation, in a recovery plan (Scully, 2011).

Transition

Section 1 contains an introduction to the study. The section includes the background of the problem, problem statement, purpose statement, nature of the study, research question, interview questions, conceptual framework, operational definitions, and the significance of the study. Additionally, Section 1 includes a discussion of the assumptions, limitations, and delimitations of the study. The last part of the section includes a literature review focusing on current cybersecurity literature. Section 2 includes the discussion of the role of the researcher, participants of the study, research method, and design, population and sampling, ethical consideration in the research, data collection, organization techniques, and data analysis technique. Section 3 will include a presentation of the findings, the application to professional practice, the implications for social change, recommendations for action, recommendations for further research, reflections and a conclusion of the study.

Section 2: The Project

The intent of Section 2 is to define the research process that I used in this study. Section 2 includes the discussion of the role of the researcher, participants of the study, research method and design, population and sampling, ethical consideration in the research, data collection and organization techniques, and the data analysis technique. Section 2 also includes information that may help future researchers replicate the study, validate the processes used to gather data, and the analysis of the data used in the study.

Purpose Statement

The purpose of this qualitative case study was to explore strategies business managers in defense contracting use to fill cybersecurity positions. The population for the study included business managers with cybersecurity responsibilities in Hampton Roads, Virginia, which is in the southeastern region of the state.

I used purposeful sampling, which resulted in a sample size of eight participants from which I gathered data. The sample size may seem limited, but Robinson (2013) suggested a sample size of three to16 participants is ideal for small-scale, interview-based qualitative research. The contribution to social change is to provide organizations with an understanding of the best strategies to fill cybersecurity positions with cybersecurity professionals with the knowledge, skills, and attributes necessary to defend the organization’s networks and information systems.

Role of the Researcher

While conducting the study, I was responsible for the development of the semistructured interview questions, identifying and inviting prospective participants to be interviewed, administering the collection of the data in interview sessions, structuring the results for analysis, and analyzing the results. As a practicing IT professional working in the field since 2004, I was an insider researcher. Insider researchers work in the studied field (Unluer, 2012).

I hold the following professional certifications: Certified Information Systems Professional (CISSP), Certified Information System Auditor (CISA), Certified Ethical Hacker (CEH), EC-Council Certified Security Analyst (ECSA), Certified Penetration Tester (CPT), Certified Network Defense Architect (CNDA), Linux +, Security +, and Network +. I am an adjunct assistant professor at an online college in the cybersecurity department.

There was no relationship between myself and the participants before the study. This ensured the anonymity and confidentiality of the research participants. I have a personal relationship with the area because Hampton Roads is my home. I set aside any preconceptions regarding the topic in order to ensure that the questions were unbiased and that the participants could express themselves freely. Recording the interviews ensured data used for analysis was accurate, and guarded against my personal perceptions when identifying thematic categories (Petty et al., 2012).

A researcher’s ethical responsibility, according to the Belmont Report protocol, is to provide respect, beneficence, and justice to each participant (Brakewood & Poldrack, 2013). Respect for participants ensures that the participants can make autonomous decisions. Participants without the ability to make autonomous decisions need protection.

All participants in this study had the ability to choose whether or not they would participate in the study. The participants had the option to exit the study at any time. Beneficence in research is not bringing harm to persons or the participant's reputation during the research process (Brakewood & Poldrack, 2013). Beneficence for the study was the assurance of protection for collected data by using encryption on the universal serial bus (USB) used for data storage and the storage of the USB in a fireproof safe. Justice in research is the balance of give and take between the researcher and the participant (Brakewood & Poldrack, 2013). I exhibited justice in the study by offering each participant a Visa gift card, usable at any merchant accepting Visa.

I used semistructured interview questions to guide the interview sessions for the study. The development of the interview protocol derived from information found in a variety of scholarly literature focusing on the qualitative method (Jacob & Furgerson, 2012; Torrance, 2012; White, Oelke, & Friesen, 2012). An explanation of the protocol is in the data collection section of the study. I transcribed interviews, prepared the data for qualitative data analysis, and conducted content analysis to identify thematic categories to answer the research questions.

Participants

Purposive sampling is used to identify prospective participants who could contribute to addressing the research question (Barratt, Ferris, & Lenton, 2014; Petty et al., 2012; Walker, 2012). Given the limited number of samples gathered in the study, using only experts in the field was critical (O'Reilly & Parker, 2013; Petty et al., 2012; Walker, 2012). The participants were cybersecurity professionals in management roles that work for DoD contracting companies. The study included business managers from DoD cybersecurity contracting companies in Hampton Roads, Virginia. A signed informed consent form was necessary to schedule the interview session. I worked with the participants to determine a convenient time and location for the interview, per the protocols suggested by Jacob and Furgerson (2012), Leedy and Ormrod (2013), and Petty et al. (2012).

Research Method and Design

The three main research methods in the social sciences are: quantitative, qualitative, and mixed methods (Walker, 2012). Each of the methods has strengths and weaknesses. Choosing the method with the best opportunity to answer the research question is important. The research method guides the research in a systematic process for producing quality, credible research. The researcher should also pay attention to the process for each method and be prepared to execute the actions required for the chosen research method (Petty et al., 2012).

Research Method

Quantitative researchers use quantitative methods when there is a need to investigate current conditions, relationships of variables, and the cause and effect of certain phenomena (Mustafa, 2011). However, for this study, the purpose was to explore the perceptions and experiences of business managers in DoD contracting companies filling cybersecurity positions. A lack of verified survey instruments for the research topic prevented the use of the quantitative method.

A mixed methods approach is a combination of the traditional qualitative and quantitative methodologies (Denzin, 2012; Venkatesh, Brown, & Bala, 2013). Mixed methods methodology did not align with this study because the intent of the study was to explore successful strategies used to hire cybersecurity professionals for DoD contracts, not to quantify the existence of this behavior. The quantitative element of the mixed methods research made the mixed methods approach inappropriate for the study because of the lack of verified survey instruments for the research topic.

The purpose of qualitative research, as explained by Denzin (2012), is to make a positive difference and be the catalyst for social change. Using the qualitative method allows the researcher to analyze the perceptions of participants about an event or phenomena (Houghton, Casey, Shaw, & Murphy, 2013; Petty et al., 2012; Walker, 2012). The qualitative method was suitable for the study because the focus is on analyzing the perceptions of study participants regarding filling cybersecurity positions for DoD contracting companies. Qualitative research involves perspectives and experiences of people in the setting the phenomena or problem exists. Qualitative researchers use multiple data sources and data collection techniques to gather the information needed (Denzin, 2012).

Research Design

There are different approaches within the qualitative method. The chosen approach should focus on applying an existing theory to a business problem and not developing new theories. The researcher should use their worldview as the lens used to explore the research question (Denzin, 2012). Three qualitative research approaches are appropriate for a doctoral study. The three potential designs are a phenomenological inquiry, ethnographic analysis, and case study analysis. Each design offers benefits and disadvantages a researcher should consider when choosing the design.

In a phenomenological study, the researcher examines the lived experiences of a group of research participants in an attempt to understand the concept or the phenomenon under inquiry (Walker, 2012). A researcher will use a phenomenological design if their intent is to explain how the phenomenon studied can improve an aspect of the business or the organization. The intent is to capture the uniqueness of the phenomenon (Petty et al., 2012). The phenomenological design was not suitable for this study because the participant pool in one organization is not large enough to attract the 20 participants required for the study.

In an ethnographic study, the researcher gathers data in order to understand the cultural patterns of a group (Petty et al., 2012). An ethnographic study would be a good approach for a researcher with the ability to become a part of the culture under inquiry in order to understand the problem. Becoming a part of the culture can introduce bias if the researcher does not remain neutral, but getting the firsthand knowledge of the people in the group may help the researcher gain an understanding of the problem (Burghardt et al., 2012). The ethnographic analysis design was not suitable for this study because it does not seek to gain knowledge about the cultural patterns of cybersecurity professionals.

A case study design aligned with the intent of the study because the case study uses several different forms of data gathering methods to capture the information needed to understand the problem (Walker, 2012). Case study research is a detailed exploration of a phenomenon in a real-world scenario (Yin, 2013). Collecting data from multiple sources adds credibility to the researcher and the conclusions reached in the study (Houghton, Casey, Shaw, & Murphy, 2013).

Case study research design provides an in-depth look at an individual or small participant pool (Petty et al., 2012), with an emphasis on exploration and description (Yin, 2013). According to Houghton et al. (2013), the case study design allows the researcher to have more flexibility in data collection. Houghton et al. posited that the researcher adapts according to the data. In addition, Petty et al. (2012) posited the intent case study research design is to explore the events and behaviors resulting in the occurrence of a certain condition.

Researchers use various techniques to collect data with the ultimate goal of exploring the human perspective (Jacob & Furgerson, 2012). Interviews allow open communication between the researcher and the participant (Anyan, 2013). I decided that a case study design was appropriate for the current study because the participant and I had open and direct communication through semistructured interview responses that helped me understand the perceptions of the participants.

When the responses of the participants begin to become repetitive, data saturation is complete (Walker, 2012). I reached data saturation by using purposive sampling to interview eight participants. The eight participants provided enough information to complete the study.

Population and Sampling

The target population for the study included business managers with cybersecurity responsibilities. Specifically, the participants were professionals working in a managerial role in the field of cybersecurity for DoD contracting companies in a Hampton Roads, Virginia. Participants participated if they signed the consent form and worked in a cybersecurity hiring manager role for a DoD contracting company. I sought a minimum of eight participants from two groups of cybersecurity professional organizations in Hampton Roads, Virginia. I found eight participants that represented eight different companies. The reason for using different companies to collect data from companies across the DoD contracting industry in Hampton Roads, Virginia.

A purposive sampling technique provides assurance the selected participants in the study are experts in the field of cybersecurity. Purposive sampling generates a small sample size (Barratt et al., 2014), but the researcher should conduct as much data gathering as necessary to reach the theoretical data saturation point (Robinson, 2013). According to O'Reilly and Parker (2013), sampling in qualitative research should focus more on the adequacy of the data collected than the amount of data collected.

In case study research, the researcher conducts an in-depth exploration of a narrowly defined phenomenon known as a case (Yin, 2013). In the study, the participants were cybersecurity managers with memberships to information systems security organizations in Hampton Roads, VA. After receiving approval from IRB, I was able to solicit eight participants from the organizations, and the eight participants were enough to reach data saturation.

Ethical Research

The study involved human participants. Before conducting data collection, I obtained Institutional Review Board (IRB) approval from Walden University ensure data collection procedures and techniques utilized in the study were appropriate and did not violate any protocols. The IRB approval number for the study is 06-21-16-0226851. An informed consent form was provided to prospective participants before scheduling and participating in an interview as recommended by Jacob and Furgerson (2012). A copy of the consent form is in Appendix B. To enhance anonymity, changed the names of people and organizations mentioned in the interview and modified the participant's title to obfuscate the participant's identity. Participants had an opportunity to change or modify any data after the audio transcription was complete. The participants received an opportunity to add a statement in the consent form describing additional protection measures as described by Saunders, Kitzinger, and Kitzinger (2015). During the data analysis phase, the process to identify participants was to use codes (e.g., P1, P2,). Participants refrained from providing any personal information such as name and address or other pertinent information, which may identify the participant (Saunders et al., 2015).

An encrypted USB with all collected data was stored in a fireproof safe, and the USB will remain in the fireproof safe for 5 years. Participants could withdraw from the study at any point in time without consequences. If the participant decided to withdraw, the participant could do so by voicing the withdrawal directly. A withdrawal folder on the encrypted USB will house all the data from withdrawing participants. No participants choose to withdraw from the study. The incentive for participation is a $20 VISA gift card.

Data Collection Instruments

The current study utilized the interview approach for data collection. Interviewing requires the researcher to be the primary research instrument (Chenail, 2011). The intent was to develop semistructured interview questions to assist in the interview sessions. Semistructured interview sessions allow participants to express themselves freely while ensuring the interviewer has a well-guided line of questioning (Anyan, 2013; Elo et al., 2014; Ryan & Bernard, 2003). The basis for semistructured interview questions was the perceptions and experiences of cybersecurity managers. The questions supported and addressed the research question in the study. The semistructured questions consisted of open-ended questions, which enabled the participants to express the experiences and thoughts about filling cybersecurity positions. The interview questions assured the data gathered from the participants are sufficient to cover all aspects of the topic. When the answers given by the participants become repetitive, data saturation is complete (Walker, 2012). The eight participants provided the information needed to achieve data saturation.

The implementation of the research procedures began once IRB approved the proposal. Prospective participants received an invitation letter from the representatives of the security organization. After prospective participant identification, the participant and I agreed on convenient time and place for the interview. The participants completed the informed consent form before participating in the study. The informed consent indicated the information about the study providing the participants with an understanding of the research before participation in the study. Furthermore, the informed consent form informed the participants of their right to withdraw at any time from the study.

Accordingly, the participants returned the informed consent form before the interview. The interviews were conducted face-to-face with each of the participants. Semistructured interview questions guided the interview. The semistructured interview questions allowed data collection, in which the researcher become the instrument for collection. In qualitative research, the researcher can leverage everything from paper to high tech tablet computers to record data (Wilcox, Gallagher, Boden-Albala, & Bakken, 2012). The process to ensure accuracy during transcription was to record the interview session.

Data Collection Technique

The process for data collection used in the study were interviews and a review of related job postings. The interview questions solicited responses, which reflect the experiences of business managers with input in hiring cybersecurity professionals. The participants and I meet for face-to-face interviews. Face-to-face interviews are the preferred method because face-to-face interviews allow the researcher to gather direct information from the interview questions and the researcher can gather nonverbal information from participant simultaneously (Vogl, 2013). Face-to-face interviews also build trust between the researcher and the participant (Robinson, 2013).

After receiving approval from IRB, solicitation for participation emails went to the addresses listed on the home page of two organizations. The responder of the first organization reported the intent to discuss the solicitation with the president of the organization, but the responder never replied. The second organization invited me to attend the organization's monthly meeting to network with the members to find participants for the study. Four participants agreed to participate in the study. After each interview, participants provided the names of potential participants. Four potential participants agreed to participate in the study. A copy of the contact letter is in Appendix C.

Identified participants should receive a copy of the consent form (Anyan, 2013; Chenail, 2011; Robinson, 2013). Participants of the study received a copy of the consent form after the interview. The researcher and the participant established a date and time to conduct the interview a face-to-face interview. The interview started with a script produced by the researcher. The script, located in Appendix E, was a guide for the execution of the interview. The script included an introduction the interviewer, information about the study, the process of the study, the interview questions, and information about the process after the interview is complete. The next step was to conduct the interview. The interview questions are in Appendix A. I recorded the participants' response during the face-to-face interview using a recording device.

The interview ended with a script thanking the participant and restated the measures the researcher will use to protect the participant's identity. After the interview transcription was complete, the participant received an emailed a copy of the transcribed interview for review. Participants received a copy of the transcript to check for accuracy, which is a technique known as member checking (Jacob & Furgerson, 2012; Petty et al., 2012; Torrance, 2012). A copy of the interview protocol is in Appendix D.

The second form of data collection for analysis will be a review of job postings for cybersecurity positions from the companies represented by the interviewed managers. The purpose of reviewing job postings is to gather information about the knowledge, skills and attributes hiring managers are requesting for potential new hires. After each interview, I used indeed.com and dice.com to find current job postings for cybersecurity professionals in the participant's organization and found 15 current job postings between the eight companies represented by the participants. The information in the job postings confirmed parts of the hiring process discovered through the interviews.

Data Organization Technique

There are several techniques used to organize and categorize the data for the study. Mendeley© desktop is the software used for literature organization. Mendeley© is a free pdf organizer used to save all literature in one central repository. Data collected from participants was stored in Keep Note©. Keep Note© is a tool used to save and categorize information. Each participant had a dedicated section in Keep Note©. The section included a copy of the consent form, the transcribed interview responses and any notes the researcher collected about the participant. A copy of all collected data for the study is on an encrypted USB drive which will be in a fireproof safe for 5 years.

Data Analysis

Coding, content, or thematic analysis is a method used to analyze data (Ryan & Bernard, 2003). Indulska, Hovorka, and Recker (2012) described coding as a methodological process producing a translation of the data to a higher conception level. Two levels define the codes used in the study (Oleinik, 2011; Ryan & Bernard, 2003;

White et al., 2012). The first level is the initial coding. The initial coding process produces themes easily extract from the data. Some of the codes may be words directly from the transcribed data. The second level of coding proceeds to connect level one code to increase the conceptual level of the data. Ryan and Bernard (2003) defined a theme as a recurring highlight in the analyzed data.

The data analysis process included the use of qualitative data analysis software called HyperRESEARCH to identify the frequency of occurrence of statements, which identifies thematic categories. HyperRESEARCH helped to analyze objectively the qualitative data gathered through interviews. The researcher should look for: repetitions, indigenous typographies and categories, metaphors and analogies, transitions, similarities and differences, linguistic connectors, missing data and theory related material (Ryan & Bernard, 2003). The last part of the process was to determine if the themes were valid. The use of triangulation assures the validity of the study (Bekhet & Zauszniewski, 2012; Torrance, 2012; Yin, 2013). I used information gathered from job postings as a part of the triangulation process.

The purpose of triangulation is to add validity to the research (Bekhet & Zauszniewski, 2012; Yin, 2013). Triangulation can be simple or complex in nature. A simple form of triangulation would be scaling (Jick, 1979). Scaling involves the quantification of qualitative measures. However, scaling is a primitive method of triangulating data, which does not effectively incorporate a mix of independent methods. A second method discussed and labeled as primitive is the use of field observations when used to strengthen quantitative research. The within method of triangulation uses different techniques to gather and analyze data (Jick, 1979).

The intent of using triangulation is to account for the weaknesses in the methods used (Jick, 1979). The use of three alternate techniques to analyze data will not show validity in the research unless the researcher mentions how one technique compensates for the shortcomings of one of the other techniques (Jick, 1979). Results from triangulation can be difficult to replicate, and the triangulation process will not help the research if the researcher explores the wrong research question. A comparison of transcribed interview themes and job listing themes determined whether the organization's requirements from hiring managers and requirements in job postings are the same.

A method for triangulation is the within method (Bekhet & Zauszniewski, 2012; Jick, 1979; Oleinik, 2011). The method of triangulation used in the study was the with-in method. The with-in method uses two forms of data collection with-in the same research method (Bekhet & Zauszniewski, 2012). For the study, the two forms of data collection were interviews from participant interviews and job postings from the participant’s organization.

Reliability and Validity

Four categories comprise the reliability and validity of the study: (a) dependability, (b) credibility, (c) transferability, and (d) confirmability. Recording interviews increase dependability and create an audit trail of data collected for the study. The researcher used a computer program to aid in data analysis. Participants should review transcribed interviews to verify the accuracy of the transcription (Elo et al., 2014; Houghton et al., 2013; Petty et al., 2012). The researcher gave the participant a copy of the transcribed interview to make sure the data ensure the accuracy of the transcribed data. Triangulation during data analysis and member checking after the analysis was the means to provide confirmability (Elo et al., 2014; Houghton et al., 2013; Petty et al., 2012).

The process to obtain transferability was the use of semistructured interview questions. Semistructured interview questions ensure consistency in the process of data collection for all participants. Moreover, semistructured interviews ensure future studies can replicate the data collection conducted in the study (Elo et al., 2014; Houghton et al., 2013; Petty et al., 2012).

Finally, to ensure confirmability, I used triangulation method with the data collected from interviews and job listings. The participants will receive a copy of the findings to review for accuracy if requested. The goal was to reach data saturation by using purposive sampling with a minimum of eight participants. Repetitive answers are the indicator of data saturation (Walker, 2012).

Transition and Summary

Section 2 includes the discussion of the research process. Specifically, I explain the role of the researcher, participants of the study, research method, and design, population and sampling, ethical consideration in the research, data collection, organization techniques, and data analysis technique. Section 3 will include a presentation of the findings, the application to professional practice, the implications for social change, recommendations for action, recommendations for further research, reflections and a conclusion of the study.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The purpose of this qualitative case study was to explore strategies business managers in defense contracting used to fill cybersecurity positions. The population for the study included eight business managers with cybersecurity responsibilities in Hampton Roads, Virginia. This section includes a discussion of the findings discovered through the qualitative analysis of data from semistructured interview questions and job postings from the organizations represented by the participants.

General Analysis Process

Data used in the study were collected as a result of the following semistructured interview questions:

1. How did you find skilled/qualified cybersecurity professionals?
2. How close is the training potential cybersecurity hires receive to what your organization requires?
3. What are the strengths in your hiring process?
4. What are the weaknesses in your hiring process?
5. What training opportunities does your organization offer to prepare future cybersecurity professionals?
6. What levels of education and or training do you think cybersecurity professionals need to become efficient in your organization?
7. What are the threats to your organization when cybersecurity professionals in your organization do not have the required training?

8. How does your organization ensure the cybersecurity staff has the necessary training?
9. What makes a better cybersecurity professional certification, education or both and why?
10. What additional information can you provide to assist me in understanding the phenomenon?

Eight participants responded to each interview question, offering valuable strategies on filling cybersecurity positions in DoD contracted companies. In addition to interview questions, a detailed review of 15 job postings from the organizations presented by the participants aided in broadening my perspective on recruitment processes. The review of job descriptions strengthened my understanding of the roles of cybersecurity personnel and highlighted the skillsets and experience required to fill these critical positions properly. Data drawn both from the interviews and job descriptions formulated the themes used to successfully fill cybersecurity positions.

The data analysis process included the use of qualitative data analysis software called HyperRESEARCH to identify the frequency of occurrence of statements, which aided the identification of thematic categories. I used HyperRESEARCH to analyze objectively the qualitative data gathered through interviews and job postings. Transcribed interviews and copies of the job postings were loaded into the software. Each document was labeled with unique labels to avoid duplication and to ensure each transcription and job posting were matched with the correct participant and the correct company. In the analysis I looked for: repetitions, indigenous typographies and categories, metaphors and analogies, transitions, similarities and differences, linguistic connectors, missing data, and theory related material. Each data point received an initial code. In the next stage of analysis, the initial codes were analyzed to connect level one code. Connecting level one codes increases the conceptual level of the data (Ryan & Bernard, 2003). By combining the interview question responses and secondary data used, a review of the literature, and the conceptual framework guiding the study, I developed key concepts that underscored the core requirements for successfully recruiting cybersecurity personnel. Through the process of analysis of the interview data, literature review, conceptual framework, and job descriptions, two themes evolved that may provide insight into successfully filling cybersecurity positions for DoD contracting companies. These themes were: (a) maintaining contractual requirements, and (b) a strong recruiting process.

Presentation of the Findings

The central research question guiding the study was: what strategies do business managers in United States DoD contracting companies use to fill cybersecurity positions? The research findings revealed the strategies used by hiring managers when hiring cyber security professionals for DoD contracts. As a result of the analysis of findings, two main themes evolved: (a) maintaining contractual requirements, and (b) a strong recruiting process.

Theme One: Maintaining Contractual Requirements

Overview. The first theme identified was maintaining contractual requirements. The literature does not specifically include information regarding strategies for hiring cybersecurity professionals for DoD contracts. Literature concerning contracting with the

U.S. government in general mentions the accountability mechanisms in place to ensure contract requirements are met and the repercussions of not meeting the requirements (Girth, 2014).

Organizational learning was used by 100% (8/8) of the organizations represented in the study during their hiring process. The hiring managers I interviewed used the organizational learning concept of double-loop learning, as discussed in the conceptual framework, by evaluating the requirements and subsequently changing the hiring process to meet the contractual requirements. Through data analysis, I found that maintaining contractual requirements is an important strategy when hiring cybersecurity professionals for DoD contracts. This finding answers the research question by reveling a strategy used to successfully hire cybersecurity professionals for DoD contracts.

The conceptual framework that I used in this study, organizational learning developed by Argyris, directly relates to maintaining the contractual requirement theme. Learning is a responsibility of leadership (Argyris, 1976). The hiring managers interviewed in this study are responsible for learning in the hiring process of the organization that employs them. One method of learning discussed by Argyis is single-loop learning. Single-loop learning is a learning style explained in the organizational learning theory, which reacts to a precondition (Argyris, 1976c). Contracting resembles single-loop learning because the organizations bidding for the contract receive a list of requirements to bid against. In contracting, the organization reacts to the requirements (preconditions) by hiring cybersecurity professionals with the correct qualifications for the position. In the hiring process, the organization has a checklist in the form of contract requirements to follow when filling positions for the contract. This process may yield qualified candidates based on the requirements. The process does not take into account qualities such as work experience and the candidate’s personality.

Previous researchers have paid little attention to the process of hiring cybersecurity professionals for DoD contracts. Literature regarding government service contracts in general includes studies about outsourcing and contract accountability. Girth, Hefetz, Johnston, and Warner (2012) found that government contracts at all levels are not competitive. The lack of competition increases the contracting companies’ bargaining position and allows the contracting company to charge more for the services provided (Girth et al., 2012). Girth (2014) examined how the government holds contracting companies accountable. The findings from this study may extend the knowledge into this researched topic and may motivate a deeper investigation into business accountability.

Interview Findings. The first method of data collection used in this study was face-to-face interviews. The interview questions were semistructued questions, which can be found in Appendix A. The interview questions solicited responses that reflect the experiences of business managers with input in hiring cybersecurity professionals.

Table 1

Participant's Contractual Requirement Statements

Participants	Comments
P1	We have a great grasp of what the government is looking for based on the contracts we go after.
P2	We provide what the contract needs because we understand what they want
P3	…have to make sure they fit as far as certs and education to make sure we can hire them.
P4	…potential hire always meets the requirements…
P5	Sometimes they don't really know what they want, but we provide what they asked for based on the RFP.
P6	For contract purposes, almost everyone needs a degree or a complimentary number of years.
P7	Contractually, most of the time they need to have a degree in a cyber-related field.
P8	They need to have 4 years of college and a certification that meets the government requirement for the position.

During the interviews, 100% (8/8) of the participants said that contractual requirements are the baseline for hiring cybersecurity professionals. As examples, participant 4 stated ". . . potential hire always meets the requirements . . ." Each candidate must fit the requirements of the position the government needs to fill. Participant 1 stated, "We have a great grasp of what the government is looking for based on the contracts we go after." The contracting company will offer employment to qualified candidates with the requirements located in the request for proposal.

The participants did not mention *experience* in the contractual requirements. This detail is significant because 100% (15/15) of the job postings that I evaluated contained either a specific level of experience requirement or a certification that required experience before the candidate would qualify for the position. Cybersecurity positions require years of IT-related training to implement the tactics and techniques to defend information systems effectively (Burley et al., 2014). Advanced cybersecurity certifications such as the CISM and CISSP require a minimum of 5 years of experience in one or more the knowledge domains (ISC, 2016). Cybersecurity professionals with the correct experience, training, and education qualify for cybersecurity contracting positions.

Table 2

Participant's Over Qualification Statements

Participants	Comments
P3	It can be hard to keep overqualified people because they are always looking for the next highest paying job.
P5	. . . they have more than what we need for the contract. They tend to get bored and find something that pays more and offers more non-routine work.
P7	We try not to train them up too much because they may leave us after we pay for their training
P8	They seem to work out for a while, but we lose a good deal of them because they find jobs where they can make more money doing the same job.

Half of the participants (4/8) expressed their reluctance to hire overqualified candidates to fill positions because overqualified candidates may leave the contract early if a more lucrative position is available at a future date. As examples, Participant 3 stated, “It can be hard to keep overqualified people because they are always looking for the next highest paying job.” All the participants (8/8) stated that underqualified candidates do not proceed beyond the screening process. Participant 7 stated "[We] can’t hire a person that does not have the basic qualifications.” Participant 5 stated “If they don’t have the training, we can’t hire them. It’s that simple.”

Table 3

Training Requirements for Contract Compliance

Participants	Comments
P1	We have annual training requirements. Some are for compliance others are for refresher training. We also do brown bag training sessions where we use our lunch time to review skills.
P2	We do the government training as required.
P3	Everyone on staff has a training profile, and we make sure we keep it up to date.
P4	Once they are hired we make sure they have a chance to get as much training as we can afford and that they need.
P5	When there are new requirements for the contract, we try to get them the training
P6	…for the required government training. We get that done on time because we have to.
P7	We do annual training.
P8	We have some government requirements that we have to adhere to and we do those.

One contractual requirement underscored by 100% (8/8) of the participants was the need for continuous training. Training regiments for cybersecurity professionals depend on the type of cybersecurity program, but the goal is to have a defined set of training objectives across the cybersecurity discipline (McGettrick, 2013). All of the participants, 100% (8/8), indicated that the DoD required contractors to do annual security training. The training is user-level training, but the training is the only requirement the contract requires the company to complete. Meeting this requirement is an example of single-loop learning.

Table 4

Continuous Training to Meet Certification Requirements

Participants	Comments
P1	We also have a tailored training budget designed to provide training
P2	…and we get our people training for their certifications. That is used as a retention tool because some of those certs cost close to $100 a year.
P3	…cert training is on an individual basis, but we give our employees the space to choose what they want to do as far as training
P4	We pay to keep the certifications training up. It can get expensive, but we have to do it to keep our employees happy.
P5	If timing allows us and we have the funds, we try to send them to training for places like SANS, to conferences like ShmooCON, or to one of the other training centers around town.
P6	…cert training is basically done haphazard - there is no training budget, no continuing education program - everything is on an individual basis…but it has to get done
P7	…we allow our employees to do free online training during their regular work hours to support them getting the training they need.
P8	We lean on free courseware like Cybrary and cheap courses from Udemy to keep up with certification training

The other training discussed by 100% (8/8) of participants was certification training required by cybersecurity certification organizations. Addressing the need for training and allocating the necessary resources is a high priority for organizations worldwide (Hoffman et al., 2012). The two small companies did not have a training budget to support paying for training. As an example, participant 7 stated, “We allow our employees to do free online training during their regular work hours to support them getting the training they need.”

The larger companies have the training budget to support the training of their cybersecurity professionals. Larger companies, which encompassed 75% (6/8) of participants, have training budgets large enough to support outsourcing cybersecurity workforce training by allowing employees to attend security training at local training centers and security conferences such as BlackHat and ShmooCON. Participant 5 stated, “If timing allows us and we have the funds, we try to send them to training for places like SANS, to conferences like ShmooCON, or to one of the other training centers around town.” Large organizations with big training budgets can afford to keep their employees trained. Smaller organizations also have the requirement, but they find free or cheap ways to provide training to employees. The large and small organizational leaders are practicing organizational learning. The leaders of the organization show they value the continuous education of cybersecurity professionals because the leaders are willing to have large training budgets, or the organizations, use online training companies to meet the training requirement for the employees.

Table 5

Maintain Reputation by Meeting Requirements

Participants	Comments
P1	Some of the threats are developing a bad reputation, mainly through poor technical skills…
P2	The government gives us 6 months to get our people trained according to their standards. If we don’t get it done in that time, we have to let the person go and find someone else. That kills our reputation in the contracting world.
P3	…and that could hurt our ability to get future work with the units we work with now and it could make other units not want to do business with us.
P4	…is doing things that get bad reviews on our yearly contract eval. Training is one of those ankle bitters that we have to stay on top of our it will get us in hot water.
P5	…our company could lose the current contract and possibility not be considered for future contracts if we don’t keep our people trained.
P7	Basically we are in danger of losing the recompete for the contract. We have to meet all the required training goals of our client
P8	We risk not being able to do the job when our folks are not trained. That makes us look bad. Looking bad is not good when you are a contractor.

The preponderance, 88% (7/8) of participants stated providing training is necessary to maintain the organization's reputation with the government client. Cybersecurity professionals must continuously improve their skills and cybersecurity professionals must adapt to new technology (Conrad, 2012). Participant 5 stated, “our company could lose the current contract and possibility lack consideration for future contracts if we don’t keep our people trained.” If one of the cybersecurity professionals does not complete the training or fails to remain current with their certifications, then the continuation of the contract could be in jeopardy. The participants’ organizations learned to keep their employees trained, or they run the risk of earning a bad reputation, which in turn, could limit the ability of the organization to win new contracts.

Table 6

Participant’s Statements About Experience and Personality

Participants	Comments
P1	Interviews allow us to determine if their personality fits the team and if they really have the experience they say they have in their resume.
P2	Experience can trump all of that though. If you have someone with the experience, they can be sent to training to get the certs.
P3	Experience is important, and we can tell by how they answer questions if they have it.

A few, 34% (3/8) of participants, mentioned experience and personality of the candidate as discerning characteristics to consider. As examples, participant 1 stated, “…interviews allow us to determine if their personality fits the team and if they really have the experience they say they have in their resume.” Participant 3 stated, “Experience is important and we can tell by how they answer questions if they have it.” The evaluation of the two characteristics starts at the interview part of the hiring process. The reasons given for the need to have experience and personality is the fact that their cybersecurity element works in a small team. In the team, the new hire must be able to contribute to a short amount of time. The new hire's personality must fit the culture of the team. Participant 1 stated an interview question used for each candidate in the companies interview process is "What is your online avatar and why?" One participant, 12.5% (1/8), indicated the question has many purposes including, does the candidate know what an avatar is? does the candidate find online gaming interesting? Further, the description of the avatar may reveal unspoken traits of the candidate.

While 100% (8/8) of the participants expressed a need for certification related and contractually required training, the literature may lack endorsements regarding the type and amount of training a cybersecurity professional requires to be successful. Gavas et al. discussed one method for training cybersecurity professionals. Gavas et al. (2012) indicated cybersecurity team challenges are recruitment tools for students that allow the students to participate in cybersecurity, and attract the students to the profession. Student involvement relates to the study because positions require qualified candidates with experience.

Analysis of Supporting Documentation. The majority, 88% (12/15), of job postings evaluated, underscored the requirements for each position. Ensuring the candidates are neither underqualified nor overqualified is an example of double-loop learning. Double-loop learning occurs when the process changes because of feedback from previous iterations of the process (Argyris, 1996). In this situation, the hiring managers have learned to hire cybersecurity professionals with the skills needed for the contract. Hiring managers also learned hiring underqualified cybersecurity professionals jeopardized the contract because an underqualified cybersecurity professional did not meet the requirements of the contract.

When asked question 9*, What makes a better cyber security professional certification, education or both and why?* One-hundred percent (8/8) of the participants expressed a need for both. The job postings, 100% (15/15) and 93% (14/15) respectively, indicate a requirement for both certifications and education for cybersecurity contracts with DoD. According to 34% (3/8) of the participants, education and training are a start, but cybersecurity professionals also need experience. Podhorec (2012) indicated a need for cybersecurity personnel with the technical ability and the readiness to fill cybersecurity positions in different environments. The job postings for the participant's organizations had a variety of official titles for the positions. To successfully fill the position, a hiring manager must find a cybersecurity professional that has the technical aptitude and has a willing attitude to begin work in the position.

The job postings evaluated do not explicitly state the need for certification training; however, 93% (14/15) have certification requirements. The certifications have a training requirement to maintain the certification. The job postings evaluated did not contain a requirement for annual government training.

Summary. Adhering to the contractual requirements was a theme derived from the data collected in this study. Employees exposed to organizational learning capture, distribute, interpret, and, integrate information; then, institutionalize the information (Flores et al., 2012). One result of using organizational learning is an increase in the effectiveness the decision-making process (Argyris, 1976a). The hiring managers interviewed in the study make better hiring decisions by using the information gathered to hire cybersecurity professionals with the qualifications necessary to meet the requirements of the contract.

Theme Two: Strong Recruiting Processes

Overview. The second theme identified was strong requirement processes. The literature found does not specifically include information regarding strategies for hiring cybersecurity professionals for DoD contracts. Literature concerning recruitment of IT professionals included information about the knowledge, skills and attributes required for privacy engineers (Cranor & Sadeh, 2013), the importance of matching skills during the hiring process (Hoffman et al., 2012) and possible methods for recruiting new IT personnel (Gavas et al., 2012). The majority, 75% (6/8) organizations represented by the research participants used the organizational learning concept of double-loop learning, as explained in the conceptual framework, by institutionalizing the use of third-party companies to conduct the preliminary qualification and verification portion of the hiring process. The finding answers the research question by reveling a strategy used to successfully hire cybersecurity professionals for DoD contracts

The purpose of this case study was to explore strategies business managers DoD contracting companies used to fill cybersecurity positions. For this study, eight hiring managers from DoD contracting companies were interviewed using semistructutred interview questions. The analysis of the collected data indicated strong recruitment processes is an important strategy when hiring cybersecurity professionals for DoD contracts.

The conceptual framework pillar reflected in the theme is double-loop learning. Double-loop learning occurs by changing the fundamental principles of the processes, and, subsequently, the actions in the process change (Argyris, 1996). Double-loop learning also increases the effectiveness of decision-making for leaders of the organization. (Argyris, 1976a). When hiring cybersecurity professionals, the organization uses feedback gained from previous hires to improve the overall hiring process. One learning event discussed by 62% (5/8) participants was the decision to hire outside organizations to recruit cybersecurity professionals. The participants' organizations learned what portions of the hiring process are important enough to handle personally, and what portions to outsource to an external organization. One portion of the hiring process where outsourcing is preferred is the resume review.

Recruiting was mentioned by Cranor and Sadeh (2013) when searching to hire for privacy engineers and the importance of the engineer's possessing the correct technical and problem-solving skills to successfully operate in the organization. Hoffman, Burley, and Toregas (2012) mentioned recruiting and the importance of matching skills with the position. A mismatch of skills could lead to a new hire that does not meet the requirements for the contract. Terrorist also value hiring cybersecurity professionals with the basic requirements to conduct cyber-related attacks (Hua & Bapna, 2013). Hua and Bapna (2013) indicated terrorist organizations recruit well-educated, computer literate individuals to join terrorist groups as cyber operators. The terrorist organization trains the new recruits on the specifics of the cyber position, but recruitment starts because the individual has a baseline set of skills in IT. The recruiting companies and HR departments help the organizations find and verify the qualifications of potential cybersecurity hires.

Interview Findings. The first method of data collection used in the study were face-to-face interviews. The interview questions were semistructued questions which can be found in Appendix A. The interview questions solicited responses, which reflect the experiences of business managers with input in hiring cybersecurity professionals.

Table 7

Third Party Resume Review Statements

Participants	Comments
P1	We get a lot of resumes from online job postings and a few through personal contacts.
P2	It takes us a long time to weed through those resumes to find possible candidates.
P3	They do a great job for us with the resume review and other preliminary screening for candidates
P5	I’ve been trying for years to get or company to invest in a recruiting company because of the number of resumes that we get.
P7	The screening process can be intensive. Just reviewing the resumes alone would take us days…
P8	They got us through the hard part of screening candidates…

A significant number, 75% (6/8), of participants expressed the overwhelming number of resumes received after posting a new position is the hardest to complete, but easiest to outsource to a third party. As examples, participant 1 stated, “We get a lot of resumes from online job postings and a few through personal contacts.” Participant 5 works for a company that did not use a third-party recruiter; however, the participant stated, “I’ve been trying for years to get our company to invest in a recruiting company because of the number of résumés that we get. We don't have the time to go through the résumés like we should.” Of the hundreds of résumés for each job postings, only a handful of candidates meet the requirements presented in the job postings.

A significant number, 75% (6/8), of participants used a third-party company to recruit qualified candidates. Participant 6 stated the organization used “…staffing agencies that specialize in CS-type jobs.” Participants, 75% (6/8), expressed the advantage of using a third-party company to find the right candidate to fill the position promptly. The recruiting company conducts the qualification verification for the participants. Participant 2 stated, “It takes us a long time to weed through those resumes to find possible candidates.” By outsourcing parts of the hiring process that are time-consuming, the participants and their hiring team are free to focus on the other parts of the hiring process. The change in the hiring process is an indication that the organization is using double-loop learning. Double-loop learning occurs when feedback from a process provides the catalyst to change the process (Argyris, 1996). A large portion, 75% (6/8), saw a third party recruiter as a strength because the recruiter streamlined the recruitment and vetting portion of the hiring process.

A couple, 25% (2/8), of participants in organizations that only use their internal HR department expressed the reason the organization only used the HR department was because the organization was large and the organization does not think it was necessary to hire third party recruiters to do the same function as an existing department in the organization. Participant 4 stated, “I gave HR my requirements. Then HR brought me the most qualified candidates based on my requirements.” Utilizing the HR department in the described way is an example of single-loop learning. The HR department is given a set of conditions in the form of contract requirements. Single-loop learning is one of the pillars of the organizational learning theory (Argyris, 1976b). The participants’ comments suggested the organization’s HR department is proficient in the recruitment process.

Table 8

Major Strengths in Hiring Process

Participants	Comments
P1	We have a streamlined process for hiring. There isn’t a lot of extra stuff in our process.
P2	It would have to be the recruiting company we use. [Recruiting Company] has a great process that we love. It has proven to give us the type of candidates that we need to fill our open jobs.
P3	The biggest strength is our HR department. They are all over it. After an interview, they do all the negotiations for pay and benefits in a timely manner and we usually get the candidate that we want…
P5	I think our HR department does a great job when we give them clear requirements. I would say they do a good job of picking through the applicants and figuring out who we need to give an interview to.
P7	[Recruiting Company] is our strength. Not only for what they do for us, but the fact that using them frees us up from having to deal with the finding people part. . .
P8	I would have to say it's our process. We get them in, get them interviewed and processed and we keep it the process moving.

The most notable strengths in the hiring process for the participants are the streamlined hiring process and human resources involvement. Half, 50% (4/8), of participants stated the streamlined hiring process is a strength. The four participants expressing this strength use recruiting companies to assist in the hiring process. The HR department is a strength to the two companies that use the organization's internal HR department for recruiting because the HR department is proficient in recruiting and hiring cybersecurity professionals.

Table 9

Major Weakness in Hiring Process

Participants	Comments
P2	…the weakest thing about our process is the lack of communication between us and the HR department when we choose a candidate. What I mean by that is there are a bunch of HR type things that have to happen before the candidate can start working.
P3	…the biggest problem is the time from accepting the job to the person coming to work.
P4	The process is slow. I mean really slow. I think it is because we are a satellite branch of the main organization…
P5	Working with the government can be slow and I would say they [the government] holds us up in onboarding process.
P6	For being a small company, it seems to take way too long to bring some one on board.
P8	…weakest part of the process comes from dealing with the government. They can be slow when they issue the RFP and when they go through the contracting award process. That kills us because we find good candidates, but they sometimes find a position with another company before the contract is awarded.

The weaknesses include the slow process of getting started after hiring and the lack of consideration for the personal attributes of the candidates. Slightly more than half, 62% (5/8), of the participants stated the biggest weakness in the process is the excessive amount of time used in the onboarding process. The data point is significant because the data point ties directly to organizational learning. An organization practicing organizational learning techniques view processes from an organizational view (Caldwell, 2012). Sixty-two percent of the organizations represented learned new employees might face a long wait time between the date of hire and the date they start working with the client. The organizations modified the portion of the hiring process they control to streamline the time between job posting and the candidates hiring.

Analysis of Supporting Documentation. The majority, 80% (12/15) of job postings have specific requirements for potential candidates. The 12 job postings described in detail every qualification the candidate should possess. Certifications and a college education are consistent requirements found in 100% (15/15) and 93% (14/15), of job postings respectively. A total of .06% (1/15) of the postings did not specify a degree as a requirement for the position; however, one-hundred 100% (15/15) had a specific certification requirement. The job postings did not indicate if the job posting originated from the organization’s HR department or a third-party recruiting company, but six of the eight companies used third party recruiters for portions of the recruitment process. The results suggested the participants use third-party recruiters to enhance the process for successfully filling cybersecurity positions for DoD contracts.

Summary. A strong recruiting process was a theme exposed by the analysis of the data collected for this study. A byproduct of implementing organizational learning is the ability to increase the effectiveness of decision-making processes (Argyris, 1976a). Organizations also use organizational learning to institutionalize processes (Flores et al., 2012). Of the hiring managers interviewed in this study, 75% (6/8) suggested a strong recruiting processes included hiring a third-party company to conduct the initial recruitment and verification of new hires. The finding indicated hiring managers use organizational learning to make better business decisions and to institutionalize portions of the hiring process to increase the likelihood of recruiting qualified cybersecurity professionals for DoD contracts.

Applications to Professional Practice

The two themes identified in the study show organizations contracting cybersecurity services with DoD, value maintaining contractual requirements and relying on a strong recruitment process. Contracting companies providing cybersecurity services to DoD, and contracting companies preparing to bid for contracts with DoD, may gain a competitive advantage when preparing to hire for cybersecurity positions. Organizations with current DoD contracts can use the results of the study to increase their proficiency in their hiring process. Organizations that wish to pursue DoD contracts that provide cybersecurity services may find information in the study that could help them understand the cybersecurity contracting landscape. The use of organizational learning principles helped hiring managers in each organization by aiding the organization to institutionalize maintaining contractual requirements and developing a strong recruiting process. Implementing organizational learning, maintaining contractual requirements and developing a strong recruitment process are strategies used by hiring managers to fill cybersecurity positions for DoD contracts.

In 2014, the U.S. government's budget was $3.5 trillion. $445 billion or 13% of the overall budget dedicated to contracts. The DoD received 64% of the $445 billion and DoD spent 45% of the allocated money on service contracts (Schwartz, Ginsberg, & Sargent, 2015). A company not able to fulfill their contractual requirements may find it hard to win cybersecurity contracts with DoD. The DoD allocates funds for the services they want (Schwartz et al., 2015). An example given by participant 3 was the process of purchasing a boat for DoD. If the DoD asks for a 20ft boat, the organization bidding for the contract to provide the 20ft boat must produce a 20ft boat. If the organization reviews the request for proposal and determines that the DoD needs a 35ft boat, and they provide them with the 35ft boat, they run the risk of not winning the contract. The point of the participant's story is DoD contractors that want to provide cybersecurity services to DoD must meet the contractual requirements. Meeting contractual requirements is one portion of the strategy used by hiring managers to successfully fill cybersecurity professionals for DoD contracts.

The implementation of a strong recruiting process may help organizations find the cybersecurity professionals that meet the requirements of the contract. Recruiting is an integral part of the hiring process (Strohmeier, 2013). Seventy-five percent (6/8) participants suggested having a third-party organization is more advantageous than using the internal HR department because third-party recruiters can eliminate candidates that do not meet the basic requirements for the position. The results indicate a strong recruiting process increase the operational effectiveness of the hiring process by streamlining hiring, reducing the workload for hiring managers, and increasing the likelihood of finding qualified cybersecurity professionals. Developing a strong recruitment process is a strategy hiring managers use to successfully hire cybersecurity professionals for DoD contracts.

Implications for Social Change

The results of this study may help cybersecurity professionals understand the process DoD cybersecurity contracting companies use when hiring new cybersecurity professionals. The information provided in this study may allow the new cybersecurity professional to understand what they need to do to prepare themselves for positions with cybersecurity contracting companies. Organizations with current DoD contracts can use the results of the study to increase their proficiency in their hiring process by using double-loop learning instead of single-loop learning. Double-loop learning generates concrete solutions to a problem (Argyris, 1976a).

Organizations with the desire to pursue DoD contracts providing cybersecurity services might find information in the study that could help them understand the cybersecurity contracting landscape. The study may also help organizations understand the advantages of using the organizational learning concept. Information security is not a separate function, but a subset of the strategic business security strategy for an organization (Jirasek, 2012). In cybersecurity, the stakes can be high. An attack on unprotected or poorly protected information systems can cause a loss of confidence in the institution and lower the organizations stock price (Gordon et al., 2011). Cyber criminals routinely exploit the lack of coordination between private companies and government (Quigley et al., 2015). Providing qualified cybersecurity professionals for DoD contracts can help reduce the risk of operating in cyberspace for the DoD.

Recommendations for Action

Contracting companies that provide cybersecurity services to DoD should pay attention to this study. From this study, contracting companies providing cybersecurity services to DoD and contracting companies preparing to bid for contracts with DoD may gain a competitive advantage when preparing to hire for cybersecurity positions. An advantage may develop by institutionalizing the preparation and hiring processes learned by the organization. The institutionalization builds a steady foundation the organization’s hiring process (Lengnick-Hall & Inocencio-Gray, 2013). Based on the results of the study, 100% (8/8) of the participants suggested the hiring managers need a strong understanding of the contractual requirements. All, 100% (8/8), participants suggested organizations need to develop hiring processes, which includes clear instructions from the hiring manager and a streamlined process for the candidate.

The results of the study indicate understanding the contractual requirements of the contract is the first competitive advantage because understanding the requirements ensure the organization knows what they must accomplish to fulfill the contract. The contract requirements will be in the form of a checklist. Hiring managers need to use double-loop learning techniques to increase the rate of successful hires. Without the implementation of double-loop learning hiring managers are unable to reevaluate the requirements (Argyris, 1976c). Reevaluation of the requirements will help the organization understand the status of meeting the requirements, and reevaluating the requirements will help the organization determine what processes need adjustments.

The second competitive advantage indicated in the results of the study is understanding the HR portion of the hiring process. The organizational learning process starts with employees that have the knowledge, skills, and attributes to complete the assigned tasks (Caldwell, 2012). Recruiting companies and HR departments are responsible for vetting the qualifications of the potential hires for the contract. The proper allocation of resources and capabilities is a catalyst for competitive advantage (Lai, 2012).

Hiring managers should ask, *Do I understand what the organization wants in a cybersecurity professional? Do I have the correct mechanisms in place to meet the expectations of the contract?* The ability to answer these two questions can help prepare a company to successfully hire the right personnel for cybersecurity positions. The results of the study indicate the HR department or the third-party recruiting company should consider having a clear understanding of the requirements before they release the job posting to job seekers. The reason job posting created for the position should reflect the requirements of the contract. Understanding the requirements will help find the right personnel, which in turn will help the organization build or maintain a good reputation in the DoD cybersecurity contracting industry. The results of the study may dissiminate through scholarly literature and conferences related to contracting with DoD.

Recommendations for Further Research

I conducted a qualitative case study to explore strategies used by business managers in DoD contracting companies. Limitations are weaknesses in the process used to conduct a study (Leedy & Omrod, 2013). The limitations of this study included a limited region of the U.S. and a specific focus on contracting with DoD. Hampton Roads has a large military presence; however, other government departments may offer a different insight into the problem. Further research on this topic should also focus on the value of education and certification for potential cybersecurity professionals.

All participants, 100% (8/8), stated each candidate must meet education and certification requirements. Also, 100% (8/8) expressed having certifications and a degree create an ideal level of knowledge to begin work as a cybersecurity professional. Only 25% (2/8) of participants of the organizations have intern programs that allow students interested in becoming cybersecurity professionals the ability to gain hands-on experience in the discipline. One organization made hiring students after the completion of their degree and certification requirements a priority. The concept of offering internships in cybersecurity could add value to the discussion about hiring cybersecurity professionals. Employers are reluctant to provide internships in cybersecurity because the return on investment (ROI) is hard to predict, the processes of hiring interns is expensive and organizations do not want to expose themselves to potential vulnerabilities during the training period for the intern (Hoffman et al., 2012). More research is necessary to determine the effectiveness of internships in cybersecurity.

Reflections

This qualitative case study explored successful strategies used by business managers in DoD contracting companies. I learned valuable information about the hiring process and about conducting qualitative research. The results of the study helped me to understand the difficulties of conducting qualitative research. Finding participants for a narrow case study is a challenge. The problem exists because the pool is limited. There are a finite number of companies with business managers in DoD contracting in Hampton Roads.

The data collection and analysis was exciting and rewarding. The participants came into the process with an attitude of wanting to share their experiences. I did face some difficulty finding participants, but once the first few volunteers emerged, the rest came quickly. A lesson learned is contracting with DoD for cybersecurity services is a difficult task and finding the right personnel can be a daunting process. Even with the difficulties, focused organizations with resourceful hiring managers can find ways to compete in the DoD contracting industry.

Conclusion

The Commonwealth of Virginia has 30,000 cyber-related jobs open because of the lack of skilled candidates (Day, 2014). In 2014, 54% of 17,227 cybersecurity job postings required at least one cybersecurity certification (Hughes, 2015). The purpose of the qualitative case study was to explore strategies business managers in defense contracting use to fill cybersecurity positions. The population for this study included eight business managers with cybersecurity responsibilities in Hampton Roads, VA. The process for data collection in the study was the interview method, with semi-structured interview questions, and a review of related job postings. The intent of the interview questions was to solicit a response, which reflects the experiences of business managers with input in hiring cybersecurity professionals for DoD contracting companies.

The findings of the study included two main themes leading to the successful hire of cybersecurity professionals: (a) maintaining contractual requirements, and (b) a strong recruiting process. From this study, contracting companies providing cybersecurity services to DoD and contracting companies preparing to bid for contracts with DoD may gain a competitive advantage when preparing to hire for cybersecurity positions. Organizations with current DoD contracts can use the results of the study to increase their proficiency in their hiring process. Organizations that wish to pursue DoD contracts that provide cybersecurity services will find information in the study that could help them understand the cybersecurity contracting landscape. The use of organizational learning principles helped hiring managers in each organization by aiding the organization to institutionalize maintaining contractual requirements and developing a strong recruiting process. Implementing organizational learning, maintaining contractual requirements and developing a strong recruitment process are strategies used by hiring managers to fill cybersecurity positions for DoD contracts. Further research on this topic should include other governmental departments and cybersecurity companies in other regions.

References

Abawajy, J. (2014). User preference of cybersecurity awareness delivery methods. *Behaviour & Information Technology, 33*, 236–247. doi:10.1080/0144929X.2012.708787

Alt, E., Díez-de-Castro, E. P., & Lloréns-Montes, F. J. (2014). Linking employee stakeholders to environmental performance: The role of proactive environmental strategies and shared vision. *Journal of Business Ethics*, *128,* 167–181. doi:10.1007/s10551-014-2095-x

Anyan, F. (2013). The influence of power shifts in data collection and analysis stages: A focus on qualitative research interview. *Qualitative Report*, *18,* 1–9. Retrieved from www.nsuworks.nova.edu/

Argyris, C. (1996). Crossroads--Unrecognized defenses of scholars: Impact on theory and research. *Organization Science*, 7, 79–87. doi:10.1287/orsc.7.1.79

Argyris, C. (1976). Leadership, learning, and changing the status quo. *Organizational Dynamics*, *4*, 29–43. doi:10.1016/0090-2616(76)90034-6

Argyris, C. (1976b). Single-Loop and double-loop models in research on decision-making. *Administrative Science Quarterly*, *21*, 363-375. doi:10.2307/2391848

Argyris, C. (1976c). Theories of action that inhibit individual learning. *American Psychologist*, *31*, 638–654. doi:10.1037/0003-066X.31.9.638

Barratt, M. J., Ferris, J. A., & Lenton, S. (2014). Hidden populations, online purposive sampling, and external validity: Taking off the blindfold. *Field Methods, 27,* 1–19. doi:10.1177/1525822X14526838

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information and Management, 51,* 138–151. doi:10.1016/j.im.2013.11.004

Bekhet, A. K., & Zauszniewski, J. A. (2012). Methodological triangulation: An approach to understanding data. *Nurse Researcher, 20*(2), 40–43. doi:10.7748/nr2012.11.20.2.40.c9442

Bergman, K. M. (2015). A target to the heart of the first amendment: Government endorsement of responsible disclosure as unconstitutional. *Northwestern Journal of Technology and Intellectual Property, 13,* 118-150. Retrieved from http://scholarlycommons.law.northwestern.edu

Brakewood, B., & Poldrack, R. A. (2013). The ethics of secondary data analysis: Considering the application of Belmont principles to the sharing of neuroimaging data. *NeuroImage, 82*, 671–676. doi:10.1016/j.neuroimage.2013.02.040

Burghardt, G. M., Bartmess-Levasseur, J. N., Browning, S. A., Morrison, K. E., Stec, C. L., Zachau, C. E., & Freeberg, T. M. (2012). Perspectives - minimizing observer bias in behavioral studies: A review and recommendations. *Ethology, 118*, 511–517. doi:10.1111/j.1439-0310.2012.02040.x

Burley, D. L., Eisenberg, J., & Goodman, S. E. (2014). Would cybersecurity professionalization help address the cybersecurity crisis? *Communications of the ACM, 57*(2), 24–27. doi:10.1145/2556936

Caldwell, R. (2012). Systems thinking, organizational change, and agency: A practice theory critique of Senge’s learning organization. *Journal of Change Management*, *12*, 145–164. doi:10.1080/14697017.2011.647923

Chen, H., Tan, Z., & Yang, G. (2012). Discussion on “outstanding engineers” training program for information security major in China. *IERI Procedia*, *2*, 868–872. doi:10.1016/j.ieri.2012.06.184

Chen, Y., Ramamurthy, K. K., & Wen, K. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, *29*, 157–188. Retrieved from www.jmis-web.org/

Chenail, R. J. (2011). Interviewing the investigator: Strategies for addressing instrumentation and researcher bias concerns in qualitative research. *The Qualitative Report*, *16*, 255–262. Retrieved from www.nova.edu/

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*, *39*, 447–459. doi:10.1016/j.cose.2013.09.009

Clarke, R., & Jackson, K. (2015). *Commonwealth of Virginia Cyber Security Commission*. Retrieved from https://cyberva.virginia.gov/

Clinton, L. (2015). Best practices for operating government- industry partnerships in cyber security. *Journal of Strategic Security*, *8*(4), 53–68. doi:10.5038/1944-0472.8.4.1456

Conrad, J. (2012). Seeking help: the important role of ethical hackers. *Network Security*, *2012*(8), 5–8. doi:10.1016/S1353-4858(12)70071-5

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior*, *28*, 1849–1858. doi:10.1016/j.chb.2012.05.003

Cranor, L. F., & Sadeh, N. (2013). A shortage of privacy engineers. *IEEE Security & Privacy*, *1*(2), 77–79. doi:10.1109/MSP.2013.25

Das, S. (2012). Stock market response to information security breach: A study using firm and attack characteristics. *Journal of Information Privacy & Security*, *8*, 27–56. Retrieved from www.ivylp.com/

Dawson Jr, M. E., Crespo, M., & Brewster, S. (2013). DOD cyber technology policies to secure automated information systems. *International Journal of Business Continuity and Risk Management*, *4*, 1–22. Retrieved from www.inderscience.com/

Day, B. (2014, September 4). *Cyber security commission education and workforce workgroup first meeting minutes*. Retrieved from www.cyberva.virginia.gov/

Denzin, N. K. (2012). Triangulation 2.0. *Journal of Mixed Methods Research*, *6*, 80–88. doi:10.1177/1558

Drtil, J. (2013). Impact of information security incidents–theory and reality. *Journal of Systems Integration*, *4*(1), 44–52. Retrieved from www.si-journal.org

Dunn Cavelty, M. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and Engineering Ethics*, *20*, 701–715. doi:10.1007/s11948-014-9551-y

Elo, S., Kaariainen, M., Kanste, O., Polkki, T., Utriainen, K., & Kyngas, H. (2014). Qualitative content analysis: A focus on trustworthiness. *SAGE Open*, *4*(1), 1–10. doi:10.1177/2158244014522633

Flores, L. G., Zheng, W., Rau, D., & Thomas, C. H. (2012). Organizational learning: Subprocess identification, construct validation, and an empirical test of cultural antecedents. *Journal of Management*, *38*, 640–667. doi:10.1177/0149206310384631

Furman, S., Theofanos, M. F., Choong, Y. Y., & Stanton, B. (2012). Basing cybersecurity training on user perceptions. *IEEE Security and Privacy*, *10*(2), 40–49. doi:10.1109/MSP.2011.180

Garfinkel, S. L. (2012). The cyber security risk. *Communications of the ACM*, *55*(6), 29–32. doi:10.1145/2184319.2184330

Gavas, E., Memon, N., & Britton, D. (2012). Winning cybersecurity one challenge at a time. *IEEE Security and Privacy*, *10*(4), 75–79. doi:10.1109/MSP.2012.112

Gibbins, J., Bhatia, R., Forbes, K., & Reid, C. M. (2014). What do patients with advanced incurable cancer want from the management of their pain?: A qualitative study. *Palliative Medicine*, *28*, 71–78. doi:10.1177/0269216313486310

Girth, A. M. (2014). A closer look at contract accountability: Exploring the determinants of sanctions for unsatisfactory contract performance. *Journal of Public Administration Research and Theory*, *24*, 317–348. doi:10.1093/jopart/mus033

Girth, A. M., Hefetz, A., Johnston, J. M., & Warner, M. E. (2012). Outsourcing public service delivery: Management responses in noncompetitive markets. *Public Administration Review*, *72,* 887–900. doi.10.1111/j.1540-6210.2012.02596.x

Goh, S. C., Elliott, C., & Quon, T. K. (2012). The relationship between learning capability and organizational performance: A meta-analytic examination. *The Learning Organization, 19,* 92–108. doi:10.1108/09696471211201461

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, *19*, 33–56. doi:10.3233/JCS-2009-0398

Grant, R. M. (1996). Toward a knowledge-based theory of the firm. *Strategic Management Journal*, 17, 109–122. doi:10.2307/2486994

Green, J. (2015). Staying ahead of cyber-attacks. *Network Security*, *2015*(2), 13–16. doi:10.1016/S1353-4858(15)30007-6

Hecker, A. (2012). Knowledge beyond the individual? Making sense of a notion of collective knowledge in organization theory. *Organization Studies*. *33*, 423-445 doi:10.1177/0170840611433995

Herley, C. (2013). When does targeting make sense for an attacker? *IEEE Security & Privacy*, *11*(2), 89–92. doi:10.1109/MSP.2013.46

Hiller, J. S., & Russell, R. S. (2013). The challenge and imperative of private sector cybersecurity: An international comparison. *Computer Law and Security Review*, *29*, 236–245. doi:10.1016/j.clsr.2013.03.003

Hoffman, L. J., Burley, D. L., & Toregas, C. (2012). Holistically building the cybersecurity workforce. *IEEE Security & Privacy, 10*(2), 33–39. doi:10.1109/MSP.2011.181

Hoque, N., Bhuyan, M. H., Baishya, R. C., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network attacks: Taxonomy, tools and systems. *Journal of Network and Computer Applications, 40,* 307–324. doi:10.1016/j.jnca.2013.08.001

Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigour in qualitative case-study research. *Nurse Researcher, 20*(4), 12–17. doi:10.7748/nr2013.03.20.4.12.e326

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*, 615–660. doi:10.1111/j.1540-5915.2012.00361.x

Hua, J., & Bapna, S. (2013). The economic impact of cyber terrorism. *The Journal of Strategic Information Systems*, *22*, 175–186. doi:10.1016/j.jsis.2012.10.004

Huang, C. D., & Behara, R. S. (2013). Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints. *International Journal of Production Economics, 141,* 255–268. doi:10.1016/j.ijpe.2012.06.022

Hughes, D. (2015). *BHEF 's national higher education and workforce initiative about the business-higher education forum*. Retrieved from www.cyberva.virginia.gov/

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition. *Information & Management*, *51*, 69–79. doi:10.1016/j.im.2013.10.001

Ilie, M., Mutulescu, A-S., Artene, D. A., Bratu, S., & Fainisi, F. (2011). International cyber security professionals through co-operation. *Economics, Management & Financial Markets*, *6*, 438–448. Retrieved from www.addletonacademicpublishers.com/

Indulska, M., Hovorka, D. S., & Recker, J. (2012). Quantitative approaches to content analysis: Identifying conceptual drift across publication outlets. *European Journal of Information Systems, 21,* 49–69. doi:10.1057/ejis.2011.37

Ioannidis, C., Pym, D., & Williams, J. (2012). Information security trade-offs and optimal patching policies. *European Journal of Operational Research*, *216*, 434–444. doi:10.1016/j.ejor.2011.05.050

(ISC)^2. (2016.). *CISSP-Certified information systems security professional.* Retrieved from www.isc2.org

Jacob, S., & Furgerson, S. P. (2012). Writing interview protocols and conducting interviews: Tips for students new to the field of qualitative research. *The Qualitative Report*, *17*, 1–10. Retrieved from www.nsuworks.nova.edu/

Jenkins, J. L., Grimes, M., Proudfoot, J. G., & Lowry, P. B. (2013). Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals. *Information Technology for Development, 20*, 196–213. doi:10.1080/02681102.2013.814040

Jick, T. D. (1979). Mixing qualitative and quantitative methods: Triangulation in action. *Administrative Science Quarterly*, *24,* 602–611. doi:10.2307/2392366

Jiménez-Jiménez, D., & Sanz-Valle, R. (2011). Innovation, organizational learning, and performance. *Journal of Business Research, 64*, 408–417. doi:10.1016/j.jbusres.2010.09.010

Jirasek, V. (2012). Practical application of information security models. *Information Security Technical Report*, *17,* 1–8. doi:10.1016/j.istr.2011.12.004

Julisch, K. (2013). Understanding and overcoming cyber security anti-patterns. *Computer Networks*, *57*, 2206–2211. doi:10.1016/j.comnet.2012.11.023

Kebbel-Wyen, J. (2012). Training an army of security ninjas. *IEEE Security & Privacy*, *10*(6), 91–93. Retrieved from www.computer.org/

Kim, H. B., Lee, D. S., & Ham, S. (2013). Impact of hotel information security on system reliability. *International Journal of Hospitality Management*, *35,* 369–379. doi:10.1016/j.ijhm.2012.06.002

Kim, S., Wang, Q-H., & Ullrich, J. B. (2012). A comparative study of cyberattacks. *Communications of the ACM*, *55*(3), 66–73. doi:10.1145/2093548.2093568

Kolfal, B., Patterson, R. A., & Yeo, M. L. (2013). Market impact on IT security spending. *Decision Sciences*, *44*, 517–556. doi:10.1111/deci.12023

Kostakos, V. (2012). Training users vs. training soldiers. *Communications of the ACM, 55*(3), 33–35. doi:10.1145/2093548.2093562

Kumar, R., & Singh, H. (2012). Analysis of information systems security issues and security techniques. *International Journal of Advanced Computer Research*, *2,* 65–68. Retrieved from www.theaccents.org/

Kwon, J., Ulmer, J., & Wang, T. (2012). The association between top management involvement and compensation and information security breaches. *Journal of Information Systems, 27*, 219–236. doi:10.2308/isys-50339

Lai, R. (2012). Analytic of China cyberattack. *The International Journal of Multimedia & Its Applications*, *4*(3), 37–56. doi:10.5121/ijma.2012.4304

Lengnick-Hall, C. A., & Inocencio-Gray, J. L. (2013). Institutionalized organizational learning and strategic renewal: The benefits and liabilities of prevailing wisdom. *Journal of Leadership & Organizational Studies*, *20*, 420–435. doi:10.1177/1548051812471723

Leedy, P. D., & Ormrod, J. E. (2013). *Practical research: Planning and design* (10th ed.). Upper Saddle River, NJ: Prentice Hall.

Lo, C.-C., & Chen, W. J. (2012). A hybrid information security risk assessment procedure considering interdependencies between controls. *Expert Systems with Applications, 39*, 247–257. doi:10.1016/j.eswa.2011.07.015

Lowry, P. B., Posey, C., Roberts, T. L., & Bennett, R. J. (2014). Is your banker leaking your personal information? The roles of ethics and individual-level cultural characteristics in predicting organizational computer abuse. *Journal of Business Ethics*, *121*, 385–401. doi:10.1007/s10551-013-1705-3

Maisey, M. (2014). Moving to analysis-led cyber-security. *Network Security*, *2014*(5), 5–12. doi:10.1016/S1353-4858(14)70049-2

Maughan, D., Balenson, D., Lindqvist, U., & Tudor, Z. (2013). Crossing the "Valley of Death." *IEEE Security & Privacy*, *11*(2), 14–23. doi:10.1109/MSP.2013.31

Mcdonald, J. T., & Andel, T. R. (2012). Integrating historical security jewels in information assurance education. *IEEE Security & Privacy*, *10*(6), 45–50. doi:10.1109/MSP.2012.86

McGettrick, A. (2013). Toward effective cybersecurity education. *IEEE Security & Privacy*, *11*(6), 66–68. doi:10.1109/MSP.2013.155

Mustafa, R. F. (2011). The P. O. E. Ms of educational research: A beginners' concise guide. *International Education Studies*, *4*(3), 23–30. doi:10.5539/ies.v4n3p23

Nielsen, S. C. (2012). Pursuing security in cyberspace: Strategic and organizational challenges. *Orbis*, *56*, 336–356. doi:10.1016/j.orbis.2012.05.004

Nonaka, I. (1994). A dynamic theory of organizational knowledge creation. *Organization Science*, *5*, 14-37. doi:10.1287/orsc.5.1.14

Oleinik, A. (2011). Mixing quantitative and qualitative content analysis: Triangulation at work. *Quality and Quantity*, *45*, 859–873. doi:10.1007/s11135-010-9399-4

O'Reilly, M., & Parker, N. (2013). "Unsatisfactory Saturation": a critical exploration of the notion of saturated sample sizes in qualitative research. *Qualitative Research*, *13*, 190–197. doi:10.1177/1468794112446106

Pachghare, V., Khatavkar, V. K., & Kulkarni, P. (2012). Pattern based network security using semi-supervised learning. *International Journal of Information and Network Security, 1*, 228–234. Retrieved from www.iaesjournal.com/

Paulsen, C., Mcduffie, E., Newhouse, W., & Toth, P. (2012). NICE: Creating a cybersecurity workforce and aware public. *IEEE Security & Privacy*, *10*(3), 76–79. doi:10.1109/MSP.2012.73

Petty, N. J., Thomson, O. P., & Stew, G. (2012). Ready for a paradigm shift?: Part 2: Introducing qualitative research methodologies and methods. *Manual Therapy, 17*, 378–384. doi:10.1016/j.math.2012.03.004

Podhorec, M. (2012). Cyber security professionals within the globalization process. *Journal of Defense Resources Management*, *3*(1), 19–26. Retrieved from http://journal.dresmara.ro/

Pokharel, M. P., & Choi, S. O. (2015). Exploring the relationships between the learning organization and organizational performance. *Management Research Review*, *38*, 126–148. doi:10.1108/MRR-02-2013-0033

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

Quigley, K., Burns, C., & Stallard, K. (2015). ‘Cyber Gurus’: A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. *Government Information Quarterly*, *32*, 108–117. doi:10.1016/j.giq.2015.02.001

Ransbotham, S., & Ramsey, J. (2012). Are markets for vulnerabilities effective? *MIS Quarterly*, *36*, 43–64. Retrieved from www.misq.org

Rid, T., & Buchanan, B. E. N. (2014). Attributing cyber attacks. *The Journal of Strategic Studies*, *38*, 4-37. doi:10.1080/01402390.2014.977382

Robinson, O. C. (2013). Sampling in interview-based qualitative research: A theoretical and practical guide. *Qualitative Research in Psychology*, *11*, 25-41. doi:10.1080/14780887.2013.801543

Rustici, R. M. (2011). Cyberweapons: Leveling the international playing field. *Parameters: US Army War College*, *43*(3), 32–42. Retrieved from www.carlisle.army.mil/

Ryan, G. W., & Bernard, H. R. (2003). Techniques to identify themes. *Field Methods*, *15*, 85–109. doi:10.1177/1525822X02239569

Sales, N. A. (2013). Regulating cyber-security. *Northwestern University Law Review*, *107*, 1503–1568. Retrieved from www.csuglobal.idm.oclc.org/

Saunders, B., Kitzinger, J., & Kitzinger, C. (2015). Participant anonymity in the internet age: From theory to practice. *Qualitative Research in Psychology*, *12*, 125–137. doi:10.1080/14780887.2014.948697

Scully, T. (2011). The cyber threat, trophy information, and the fortress mentality. *Journal of Business Continuity & Emergency Planning*, *5*, 195–207. Retrieved from www.ncbi.nlm.nih.gov/

Schwartz, M., Ginsberg, W., Sargent, J.F. (2015). *Defense acquisitions: How and where DOD spends its contracting dollars* (CRS Report No. R44010). Retrieved from Congressional Research Service. www.fas.org/

Smith, D. (2013). Life’s certainties: Death, taxes and APTs. *Network Security*, *2013*(2), 19–20. doi:10.1016/S1353-4858(13)70033-3

Strohmeier, S. (2013). Employee relationship management: Realizing competitive advantage through information technology? *Human Resource Management Review, 23*, 93–104. doi:10.1016/j.hrmr.2012.06.009

Suby, M., & Dickson, F. (2015). *The 2015 (ISC)2 global information security workforce study*. Retrieved from www.isc2cares.org

Torrance, H. (2012). Triangulation, respondent validation, and democratic participation in mixed methods research. *Journal of Mixed Methods Research, 6*, 111-123. doi:10.1177/1558689812437185

Unluer, S. (2012). Being an insider researcher while conducting case study. The *Qualitative Report*, *17,* 1–14. Retrieved from www.nova.edu/

Venkatesh, V., Brown, S., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly*, *37*, 21–54. Retrieved from www.misq.org

Verizon Risk Team. (2012). *Data breach investigations report.* Retrieved from www.verizonenterprise.com/

Vogl, S. (2013). Telephone Versus Face-to-Face Interviews: Mode effect on semistructured interviews with children. *Sociological Methodology*, *43*, 133–177. doi:10.1177/0081175012465967

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security professionals. *Computers & Security*, *3,* 97–102. doi:10.1016/j.cose.2013.04.004

Walker, J. L. (2012). The use of saturation in qualitative research. *Canadian Journal of Cardiovascular Nursing*, *22*(2), 37–46. Retrieved from www.ncbi.nlm.nih.gov/

Warfield, D. (2012). Critical infrastructures: IT security and threats from private sector ownership. *Information Security Journal: A Global Perspective*, *21*, 127–136. doi:10.1080/19393555.2011.652289

Warikoo, A. (2014). Proposed methodology for cybercriminal profiling. *Information Security Journal: A Global Perspective*, *23*, 37–41. doi:10.1080/19393555.2014.931491

Whitman, M. E., & Mattord, H. J. (2012). Information security governance for the non-security business executive. *Journal of Executive Education*, *11*, 97–111. Retrieved from www.citeseerx.ist.psu.edu/

Wilcox, A. B., Gallagher, K. D., Boden-Albala, B., & Bakken, S. R. (2012). Research data collection methods. *Medical Care*, *50*, S68–S73. doi:10.1097/MLR.0b013e318259c1e7

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, *37*, 1–20. Retrieved from www.misq.org

Yin, R. K. (2013). Validity and generalization in future case study evaluations. *Evaluation*, *19*, 321–332. doi:10.1177/1356389013497081

Zafar, H. (2013). Human resource information systems: Information security concerns for organizations. *Human Resource Management Review*, *23*, 105–113. doi:10.1016/j.hrmr.2012.06.010

Zarrabi, A., & Zarrabi, A. (2012). Internet intrusion detection system service in a cloud. *International Journal of Computer Science Issues*, *9*, 308–315. Retrieved from www.ijcsi.org/

.

Appendix A: Interview Questions

11. How did you find skilled/qualified cybersecurity professionals?
12. How close is the training potential cybersecurity hires receive to what your organization requires?
13. What are the strengths in your hiring process?
14. What are the weaknesses in your hiring process?
15. What training opportunities does your organization offer to prepare future cybersecurity professionals?
16. What levels of education and or training do you think cybersecurity professionals need to become efficient in your organization?
17. What are the threats to your organization when cybersecurity professionals in your organization do not have the required training?
18. How does your organization ensure the cybersecurity staff has the necessary training?
19. What makes a better cybersecurity professional certification, education or both and why?
20. What additional information can you provide to assist me in understanding the phenomenon?

Appendix B: Consent Form

CONSENT FORM

You are invited to take part in a research study that will explore the hiring gap for cybersecurity professionals in the Department of Defense (DoD). The researcher is inviting cybersecurity professionals, who work for a DoD contracting company and hires cybersecurity professionals to participate in the study. The form is part of a process called "informed consent" to allow you to understand the study before deciding whether to take part.

The study is being conducted by a researcher named Adam Pierce, who is a doctoral student at Walden University. You may already know the researcher as Adam at Jacobs Technology, but the study is separate from his work role.

Background Information:
The purpose of the research is to explore strategies business managers in defense contracting use to fill cybersecurity positions.

Procedures:

The data collection procedure is as follows:

- After I have made contact with the participant, I will send the participant copy of the consent form.
- A time and place for the interview will be scheduled.
- I will collect the consent form from the participant before the interview begins.
- We will conduct the interview which will be recorded.
- I will transcribe the audio from the interview.
- I will send the transcription to the participant so they can check it for accuracy.

If you agree to be in the study, you will be asked to:

- Meet for an interview for 60 minutes. The interview may last longer, however the researcher will guide the conversation to stay within the 60-minute time frame.
- Review transcribed responses for accuracy.
- Participate in a process called member checking, where you approve the data collected for analysis.

Here are some sample questions:

1. How did you find skilled/qualified cybersecurity professionals?

2. How close is the training potential new hires receive to what your organization requires?
3. What are the strengths in your hiring process?
4. What are the weaknesses in your hiring process?

Voluntary Nature of the Study:
The study is voluntary. Everyone will respect your decision of whether or not you choose to be in the study. No one at Walden University will treat you differently if you decide not to be in the study. If you decide to join the study now, you can still change your mind later. You may stop at any time.

Risks and Benefits of Being in the Study:
Being in this type of study involves some risk of the minor discomforts encountered in daily life, such as interrupting your daily routine, spending time away from family or other tasks after work hours. Being in this study would not pose a risk to your safety or well-being. The study has the potential to shape the view of hiring cybersecurity professionals. The study will also add to the existing body of scholarly knowledge in cybersecurity.

Payment:

All participants will receive a $20 gift card which can be used anywhere Visa is accepted.

Privacy:
Any information you provide will be kept on the researcher's personal computer is password protected. The researcher will not use your personal information for any purposes outside of the research project. Also, the researcher will not include your name or identifying information about you in the study. Data will be kept on an encrypted USB drive and the drive will be locked in a fireproof safe. Data will be kept for a period of at least 5 years, as required by the university. If illegal information is disclosed, I am obligated to report it to the appropriate authorities.

Contacts and Questions:
You may ask any questions you have now. Or if you have questions later, you may contact the researcher via email at piercea45@gmail.com or adam.pierce@waldenu.edu. If you want to talk privately about your rights as a participant, you can call Dr. Leilani Endicott. She is the Walden University representative who can discuss your concerns with you. Her phone number is 612-312-1210. You can also email her at Leilani.endicott@waldenu.edu or you can email the IRB at irb@waldenu.edu. Walden University's approval number for the study is 06-21-16-0226851 and the approval expires on June 20, 2017.

You should keep a copy of this consent form for your records.

Statement of Consent:

I have read the above information and I feel I understand the study well enough to make a decision about my involvement. By signing below, I understand and I agree to the terms described above.

Printed Name of Participant ______________________________

Date of consent ______________________________

Participant’s Signature ______________________________

Researcher’s Signature ______________________________

Appendix C: Organization Contact Letter

Dear (Organization President)

I am a doctoral student at Walden University and I am conducting a study exploring the hiring issues for hiring cybersecurity professionals. I am Certified Information Systems Security Professional (CISSP), certification number #######, and a Certified Information Systems Auditor (CISA), ISACA ID: ######. I am asking for your permission to solicit the members of your organization to participate in the study. I am looking for Eight to 15 participants. Upon completion, I am offering each participant a $20 Visa gift card which can be used anywhere Visa is accepted. Below you will find information about the procedure I will use and a few of the interview questions. There are a total of 10 questions and I will only need about an hour of the participant's time to complete the interview. The interview will be recorded to ensure accuracy. The study is voluntary. If a participant decides to join the study now, they can still change their mind later or stop at any time. I will not use the participant's personal information for any purposes outside of the research project. Also, the researcher will not include your name, the participants name or identifying information about you or the participants in the study. Being in this study would not pose a risk to your safety or well-being. The study has the potential to shape the view of future hiring of cybersecurity professionals. The study will also add to the existing body of scholarly knowledge in cybersecurity.

You may ask any questions you have now. Or if you have questions later, you may contact the researcher via email at piercea45@gmail.com or adam.pierce@waldenu.edu. If you want to talk privately about your rights as a participant, you can call Dr. Leilani Endicott. She is the Walden University representative who can discuss your concerns with you. Her phone number is 612-312-1210. You can also email her at Leilani.endicott@waldenu.edu or you can email the IRB at irb@waldenu.edu. Walden University's approval number for the study is 06-21-16-0226851 and the approval expires on June 20, 2017.

Procedures:

If you agree to be in the study, you will be asked to:

- Sign a consent form.
- Meet for an interview, for 60 minutes. The interview may last longer, however I will guide the conversation to stay within the 60-minute time frame.
- Review transcribed responses for accuracy.
- Participate in a process called member checking, where you approve the data collected for analysis.

Here are some sample questions:

1. How did you find skilled/qualified cybersecurity professionals?
2. How close is the training potential new hires receive to what your organization requires?
3. What are the strengths in your hiring process?
4. What are the weaknesses in your hiring process?

Thank you for your time,

Adam Pierce, CISSP, CISA

Appendix D: Participant Contact Letter

Dear (Participant)

I am a doctoral student at Walden University and I am conducting a study exploring the hiring gap for cybersecurity professionals working as contractors in the Department of Defense (DoD). I am Certified Information Systems Security Professional (CISSP), certification number ######, and a Certified Information Systems Auditor (CISA), ISACA ID: ######. I am looking for Eight to 15 participants for this study. For your participation, I am offering each participant a $20 Visa gift card which can be used anywhere Visa is accepted. Below you will find information about the procedure I will use and a few of the interview questions. There are a total of 10 questions and I will only need about an hour of your time to complete the interview. The interview will be recorded to ensure accuracy. The study is voluntary. If you decide to join the study now, you can still change your mind later or stop at any time. I will not use your personal information for any purposes outside of the research project. Also, I will not include your name or any identifying information about you in the study. Being in this study would not pose a risk to your safety or well-being. The study has the potential to shape the view of future hiring of cybersecurity professionals. The study will also add to the existing body of scholarly knowledge in cybersecurity.

You may ask any questions you have now. Or if you have questions later, you may contact the researcher via email at piercea45@gmail.com or adam.pierce@waldenu.edu. If you want to talk privately about your rights as a participant, you can call Dr. Leilani Endicott. She is the Walden University representative who can discuss your concerns with you. Her phone number is 612-312-1210. You can also email her at Leilani.endicott@waldenu.edu or you can email the IRB at irb@waldenu.edu. Walden University's approval number for the study is IRB will enter approval number here and the approval expires on IRB will enter an expiration date.

Procedures:

The data collection procedure is as follows:

- After I have made contact with the participant, I will send the participant copy of the consent form.
- A time and place for the interview will be scheduled.
- I will collect the consent form from the participant before the interview begins.
- We will conduct the interview which will be recorded.
- I will transcribe the audio from the interview.
- I will send the transcription to the participant so they can check it for accuracy.

If you agree to be in the study, you will be asked to:

- Meet for an interview for 60 minutes. The interview may last longer; however, the researcher will guide the conversation to stay within the 60-minute time frame.
- Review transcribed responses for accuracy.
- Participate in a process called member checking, where you approve the data collected for analysis.

Here are some sample questions:

5. How did you find skilled/qualified cybersecurity professionals?
6. How close is the training potential new hires receive to what your organization requires?
7. What are the strengths in your hiring process?
8. What are the weaknesses in your hiring process?

Thank you for your time,

Adam Pierce, CISSP, CISA

Appendix E: Interview Protocol

Interview Protocol	
Before the Interview Starts	I will ask the participant to sign/give me a copy of the consent form. Once the form has been received I will inform them that the recording is about to begin.
The start of the interview	First, I would like to thank you for participating in this study. I appreciate your willingness to participate and I hope that information we gather here will help to further our profession and professionals in our field. The interview will last approximately 60 minutes. I will ask you a series of questions to explore the topic. As stated in the consent form, your participation is voluntary. At any point, you can change your mind or stop the interview. During the interview, I may ask you to expand your response or ask follow up questions to ensure I have collected enough information.
Question 1	How did you find skilled/qualified cyber security professionals?
Question 2	How close is the training they receive to what your organization requires?
Question 3	What are the strengths in your hiring process?
Question 4	What are the weaknesses in your hiring process?
Question 5	What training opportunities does your organization offer to prepare future cyber security professionals?
Question 6	What levels of education and or training do you think cyber security professionals need to become efficient in your organization?
Question 7	What are the threats to your organization when cyber security professionals in your organization do not have this type of training?

Question 8	How does your organization ensure the cyber security staff has the necessary training?
Question 9	What makes a better cyber security professional certification, education or both and why?
Question 10	What additional information can you provide to assist me in understanding this phenomenon?
Wrap up Question and end of interview	Thank you again for your participation. In the next few days, I will provide you with a copy of the transcribed interview. I will synthesize the data based on the responses. As a part of this process, I will ask that you review the information and let me know if you agree that the information represents what you said. If there is any information that you would like me to correct or exclude please let me know.