2020

Department of Defense Insider Threats: Sharing and Oversight to Protect U.S. Installations

Yokeitha Anita Ramey
Walden University

Walden University

College of Social and Behavioral Sciences

This is to certify that the doctoral dissertation by

Yokeitha A. Ramey

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. Ian Cole, Committee Chairperson,
Public Policy and Administration Faculty

Dr. Olivia Yu, Committee Member,
Public Policy and Administration Faculty

Dr. Michael Brewer, University Reviewer,
Public Policy and Administration Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2020

Abstract

Department of Defense Insider Threats: Sharing and Oversight to Protect U.S. Installations

by

Yokeitha A. Ramey

MS, Columbia Southern University, 2007

BGS, Louisiana State University and A&M College, 1997

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

May 2020

Abstract

The growing threat of Islamic State of Iraq and the Levant and other terrorist organizations increases the Department of Defense's (DoD's) chance of encountering an insider threat, which creates the need for the DoD to develop programs to address this concern and mitigate the risk to national security. The purpose of this quantitative, nonexperimental study was to understand the effectiveness of security education, training, and awareness programs designed to mitigate insider threats within the DoD. Research questions were focused on this purpose as well as understanding why there is an increase in insider threats within the DoD. The theoretical frameworks were based on Vincent and Elinor Ostrom's institutional analysis development and Ott & Jang's theory of organizational culture and change organizational behaviors. A total of 42 DoD participants responded to a 10-question Likert-scale survey on Survey Monkey. Based on the results, the DoD needs to retain both security education, training, and awareness computer-based training and instructor-based training programs to ensure insider threats are mitigated and to prevent known acts of espionage, unauthorized disclosure, or loss of organizational resources. Implications for positive social change of these results include assisting the DoD with maintaining and developing programs to protect the warfighters and nation from terrorist threats and attacks.

Department of Defense Insider Threats: Sharing and Oversight to Protect U.S. Installations

by

Yokeitha A. Ramey

MS, Columbia Southern University, 2007

BGS, Louisiana State University and A&M College, 1997

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

March 2020

Dedication

Since the terrorist attacks on September 11, 2001, the War on Terror seems like a never-ending battle that will continue to fester for years to come. My research study is dedicated to my fellow brothers and sister in arms serving in the United States Armed Forces (Army, Air Force, Navy, Marine Corps, and Coast Guard) who have made the ultimate sacrifice of giving and risking their lives on the front lines of Afghanistan and Iraq.

A special dedication to the Gold Star families who lost loved ones serving in past and present conflicts. I want to recognize the sacrifice of these family members whose mother, father, sister, brother, son, daughter, or spouse died while serving and protecting our nation.

But the most important dedication of all is to my children. Jared and Justin, you are my inspiration. You supported me when I was deployed to Iraq and living abroad in South Korea. Although I was not there physically, you did not let my absence steer you away from your studies, because you both succeeded in school. Jared, you graduated with honors from high school. Justin, you continued to make the honor roll in preparation for your future as a cadet at one of the nation's military academies.

As the Department of Defense continues to strengthen our all-volunteer force, our nation relies heavily on the men and women on the front lines to eradicate terrorist organizations in the Middle East, Africa, and Asia to make this world a better place to live, work and travel.

Thanks for all you do! Hooah! Army Strong!

Acknowledgments

I would like to acknowledge God and my guardian angels who continue to inspire me to never give up. My brother, Dinerral Jevone Shavers, Sr. and my maternal grandparents Walter Willie and Maudrey Joyce Benton Adams. They are my inspiration and I will always keep them close to my heart.

Special thanks my mom, Yolande Adams, for her spiritual guidance, support and love which gave me the will to never to give up on my dreams.

Thanks to my sisters, Marjorica and Nakita, for sharing their words of wisdom and prayers that kept me going despite personal downfalls and medical challenges.

Jared and Justin, you are my babies and I love you. Thanks, for supporting me throughout my PhD journey and separations due to my military deployment and assignments. Now, we can travel and enjoy spending more time together.

Thanks to my aunt, Dr. Candance Russell, for reviewing my proposal and offering professional advice and recommendations for my research. You are first in the family to earn a PhD. Thanks for being my mentor and inspiration!

I would like to extend special thanks to my family and friends in New Orleans, Baton Rouge, and Denham Springs, Louisiana and the metro Detroit area who supported me throughout this journey.

Dr. Ian Cole, thanks for providing moral support and encouraging me not to give up. There were some days when I just wanted to quit, but your words of encouragement kept me going. Now, I am at the end of my journey.

Dr. Olivia Yu, thanks for making me think about why I am conducting this research. Your tough and aggressive comments during my proposal, made me a better scholar practitioner.

Ivory Hilliard, thanks for your words of inspiration, prayer and calling to check on me. Although we have not seen each other in over 20 years, you managed to make sure I was okay and stayed focused on completing my PhD.

Everett Gilliam, thanks for your love, support, and patience during my journey. Your daily inspirations and prayers got me through the day. When I was having a bad day, you always told me to be humble and to thank God for keeping me healthy and giving me life.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

Introduction

The U.S. Department of Defense (DoD) is the country's first line of defense against attacks from terrorists. If the DoD cannot stop insider threats, then it jeopardizes the organization's ability to protect U.S. citizens from acts of terrorism on U.S. soil. Recently apprehended insiders (e.g., Manning and Hasan) demonstrate America's homegrown terrorist threats to the DoD and national security (Baker, 2012). Therefore, the DoD must improve its stance on national security by thwarting insider threats. Insider threats have been identified as an issue to national security within the DoD and other government agencies (DoD, 1999).

Despite mandatory security training, education and awareness programs for military, civilian, and contractors with access to DoD resources, insider threats continue to use authorized access to harm the security of the U.S. through espionage, terrorism, unauthorized disclosure of national security information, and/or through loss or degradation of resources or capabilities (DoD, 2017b). For example, Private Bradley Manning was convicted in July 2013 of violation of the Espionage Act and other offenses after releasing the largest set of classified documents leaked to the public and was sentenced to 35 years in prison, though he was later pardoned in January 2017 and released on May 17, 2017. Additionally, the DoD identified 87% of insider threats as employees or others internal to the organization who contemplate to divulge classified information, which threatens national security (Greitzer & Hohimer, 2011). Therefore, insider threats continue to be a problem that needs to be monitored because of the current threats to national security from the Islamic State of Iraq and the Levant (ISIS) and Al Qaeda.

Deterrence is key to protecting national security, especially when DoD publicizes the consequences of misuse, abuse, and malicious activity (DoD, 1999). To accomplish the DoD's mission to protect the United States from enemies foreign and domestic, insider threats must be immediately apprehended and prosecuted (Government Publishing Office, 2016; Willemssen, 2015). However, the DoD has not identified a method or developed a system to measure the effectiveness of security education, training, and awareness programs, which are designed to ensure everyone understands the importance of identifying and reporting insider threats within their organization. The purpose of this nonexperimental, quantitative study was to understand the effectiveness of security training, education, and awareness programs as it relates to DoD personnel. Overall, researchers can assist the DoD by conducting analysis on how well education, training, sharing and oversight efforts deter insider threats.

Chapter 1 is broken down into several sections that will explain the importance of the study as well as the gaps in research. For instance, the Background section overviews the importance of the study based on related articles which exposes the DoD's vulnerabilities against insider threats. The problem statement also covers the need for the DoD to thwart and mitigate insider threats through security training, education, and awareness programs designed to ensure everyone understands the importance of identifying and reporting insider threats within their organization.

Background

The Office of the Secretary of Defense/Command, Control, Communications, and Intelligence in conjunction with the DoD must review all security related education, training, and awareness programs to mitigate insider threats (DoD, 1999). Although the DoD does not have a system or database dedicated to tracking insider events, characteristics, lessons learned, or statistics, the Carnegie Mellon's Computer Emergency Response Team (CERT) developed a database that provides information and tools to policymakers, personnel security, and security education and training directorates (DoD, 1999). Additionally, army leaders must encourage subordinates to report insider threats; however, without effective security education, training, and awareness programs in place, identifying and reporting insider threats is difficult (DoD, 1999). For example, Baker (2012) identified that the lack of these programs among Army leaders led to not identifying Major Nadal Hasan's sympathy toward ISIS and other terrorist organizations. Therefore, there is a need to improve the effectiveness of the current programs to identify, deter, and mitigate insider threats.

DoD regulations and policies were revised in 2015 to ensure personnel (i.e., military, civilian, and government contractors are provided annual security training, education, and awareness. However, the effectiveness of this training is not being measured by the DoD, which prevents military personnel, DoD civilians, and contractors from understanding the importance of identifying and reporting insider threats within their organization. The DoD is also unaware of the effectiveness of security education, training, and awareness programs in general because it has not conducted evaluations or tests through military training exercises. Further, although President Obama signed Presidential Executive Order 13587 to improve structural reforms on protecting and securing classified networks and safeguarding classified information within government agencies (Kirschbaum, 2015), government agencies and organizations, such as the DoD, struggle to improve and maintain effective security training, education, and awareness programs due to a lack of funding (Johnson, 2013). But the DoD and other agencies must be prepared to protect information, resources, and facilities from insider threats. Therefore, it is important to measure the effectiveness of such programs to ensure deterrence, identification, and mitigation of insider threats, which this study addresses.

Problem Statement

According to the United States Army 902nd Intelligence Group (2016), there are specific indicators that put an individual at risk of becoming an insider threat:

1. Encouraging disruptive behavior or disobedience to lawful order;
2. Expressing hatred or intolerance of American society or culture;
3. Expressing sympathy for organization that promote violence;
4. Expressing extreme anxiety about or refusing a deployment;
5. Associating with or expressing loyalty or support for terrorists;
6. Browsing websites that promote or advocate violence against the United States, or distributing terrorist literature or propaganda via the internet;
7. Expressing extreme outrage against U.S. military operations;
8. Advocating violence to achieve political/religious/ideological goals;
9. Providing financial or other materiel support to a terrorist organization;

10. Seeking spiritual sanctioning for or voicing an obligation to engage in violence in support of a radical or extremist organization or cause;
11. Membership in a violent, extremist or terrorist group, or adopting an ideology that advocates violence, extremism, or radicalism;
12. Purchasing bomb making materials or obtaining information on bomb construction and use;
13. Engaging in paramilitary training with radical or extremist organizations, either home or abroad;
14. Having ties to know or suspected international terrorists, extremists, radicals, or their supporters; and
15. An employee released from or not selected for employment, promotion, or bonus; who exhibits server signs of PTSD, and who appears disgruntled and violent.

Examples of insider threats include former Army Private Bradley Manning and Army Major Nidal Hasan (Koester, 2013). On May 17, 2017, Manning was released after only serving 7 years of a 35-year sentence, whereas Nidal remains on death row. The DoD identified these individuals as insider threats after Manning provided classified documents to WikiLeaks and Hasan killed and wounded soldiers at Fort Hood, Texas (Thompson, 2014).

An insider threat is an individual who can intentionally or unintentionally harm national security through acts of espionage and unauthorized disclosure of classified information causing a loss of degradation to operational capabilities and resources

(Defense Security Service Regulation, 2014). Additionally, an insider threat can negatively impact national security resulting in loss of life, compromising and disclosing classified information and systems, and causing economic loss due to the cloning or destruction of major weapons systems and loss of technology (Defense Security Service, 2014). There are several categories of insider threats: foreign agents stealing classified information, workers angry with management leaving for a new job, and greedy workers willing to engage in espionage (Magnuson & Sicard, 2015). Historically, DoD insider threats have been middle-aged males with an agenda to commit espionage and disclose classified information to foreign governments (Herbig, 2017).

After several insider threat attacks within the DoD, there is a need to improve security education, training, and awareness programs (Kirschbaum, 2015). Additionally, security experts from CERT and the Federal Bureau of Investigation (FBI) investigated insider threats in 2012 by assessing archetypes and employee impressions and found that 70% of respondents said they do not have enough information or tools to be proactive in identifying insider threats (Magnuson, 2014). Despite programs in place, the effectiveness of DoD’s insider threat security education, training, and awareness programs have not been evaluated. This study was conducted to identify the perceived effectiveness of DoD’s security education, training, and awareness programs provided to military, civilian, and government contractors to mitigate and provide oversight of insider threats.

Purpose of the Study

The purpose of this quantitative study was to understand the effectiveness of the security education, training, and awareness programs currently provided to military, civilian, and government contractors with access to DoD resources, organizations, and facilities. Although DoD has several types of security education, training, and awareness programs, this study included comparing the effectiveness of computer-based training (CBT) and instructor-based training (IBT). Institutional analysis development (IAD) and the theory of organizational culture and change guided the study as it relates to security education, training, and awareness programs of insider threats within the DoD. The independent variables were DoD CBT versus IBT programs designed to mitigate insider threats in which criterion determines whether the effectiveness of security education, training, and awareness CBT or IBT programs changes attitudes, improve knowledge or increase skills in identifying an insider threat. The dependent variables were known acts of espionage, unauthorized disclosure of information, and any activity resulting in the intentional or unintentional loss of organizational resources and/or capabilities from the actions of an insider. Control and intervening variables were gender and military and civilian status (e.g., noncommissioned officer, DoD civilian, etc.).

Research Questions

RQ1: What is the perceived effectiveness of CBT and IBT programs in mitigating and thwarting insider threats within the DoD?

$H_0$1: There is no statistically significant difference between the perceived effectiveness of CBT and IBT programs in mitigating and thwarting insider threats.

H$_1$1: There is a statistically significant difference between the perceived effectiveness of CBT and IBT programs in mitigating and thwarting insider threats.

RQ2: What is the perceived effectiveness of CBT and IBT programs in preventing known acts of espionage, unauthorized disclosure, or loss of organizational resources?

H$_0$2: There is no statistically significant difference between the effectiveness of CBT and IBT programs in preventing known acts of espionage, unauthorized disclosure, or loss of organizational resources.

H$_1$2: There is a statistically significant difference between the effectiveness of CBT and IBT programs in preventing known acts of espionage, unauthorized disclosure, or loss of organizational resources.

Theoretical Framework

IAD and the theory of organizational culture and change are the theoretical frameworks that best suit this study because both are systematic ways of studying institutional organizations and their cultural impact on organizational realities and relationships. In 1971, Vincent and Elinor Ostrom developed the IAD framework as a systematic way of studying institutional arrangements. Ostrom's IAD framework suggests the direct impact of operational decisions of decision-makers such as Army leaders (i.e., commanders, platoon leaders, senior executive service, etc.), who are required to make policy decisions within the constraints of a set of collective rules created within an organization such as the DoD. The IAD draws out assumptions about rules ranging from statutes to patterns of behavior (Sabatier & Weible, 2014).

In contrast, the theory of organizational culture and change organizational behaviors and decisions are predetermined by assumptions of members within an organization (Shafritz, Ott, & Jang, 2016). For example, research has shown an increase in insider threats within the DoD because leadership did not identify patterns of behavior exhibited by insider threats or make changes to its current culture (Baker, 2012). This led to Presidential Executive Order 13587 (Kirschbaum, 2015). Although the DoD's culture accepts the fact that changes must be implemented to prevent insider threats, they are slow to make changes because of the organizational culture of each military service (i.e., Army, Air Force, Navy, and Marine Corps) (Kirschbaum, 2015). As a result, each military service must work together to develop a tracking system based on lessons learned, after action reviews, and assessments. Presidential Executive Order 13587 was aimed to change the organizational culture by making changes to how each organization shares information on a joint database (Kirschbaum, 2015). In 2016, DoD is in the process of developing such a database, which will monitor, analyze and identify insider threats in accordance with Executive Order 13587.

Nature of the Study

The nature of this study was quantitative and nonexperimental, focused focus on the effectiveness of security training, education, and awareness and its relationship to identifying and reporting insider threats. A survey was used to assess the benefits and risks of security training, education, and awareness and its effectiveness on identifying and reporting insider threats within the DoD. The design was focused on a limited number of independent (security education, training, and awareness programs) and dependent (insider threats) variables. The independent variables were be DoD programs designed to mitigate and thwart insider threats in which criterion determines whether the effectiveness of security education, training, and awareness CBT or IBT programs changes attitudes, improve knowledge or increase skills in identifying an insider threat. The dependent variables were acts of espionage, unauthorized disclosure of information, and any activity resulting in the intentional or unintentional loss of organizational resources and/or capabilities from the actions of an insider (Defense Security Service, 2014).

The quantitative research design allowed for a statistical analysis using Two-way Analysis of Variance (ANOVA) to analyze data collected from the surveys as well as a means for determining relationships between independent and dependent variables and their effect on identifying, mitigating, and eliminating insider threats within the DoD. A comprehensive survey was used to collect data from military personnel (i.e., enlisted, noncommissioned officers, warrant officers, and commissioned officers) and government civilians (i.e., general schedule [GS] and senior executive service contractors and information technology, engineers, logisticians, etc.) from military installations across the United States. The survey was distributed electronically to participants to determine if the effectiveness of security education, training, and awareness programs helps them understand how to identify and report insider threats within their respective organizations. Thus, this study helps reflect the need to modify existing or develop new methods to identify and report insider threats within the DoD by identifying any deficiencies in the effectiveness of security education, training, and awareness programs.

Definitions

Classified information: Information that has been determined pursuant to any successor order, Executive Order 12951 or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011), to require protection against unauthorized disclosure and that it is marked to indicate its classified status when in documentary form (Defense Security Regulation 05-06, 2014).

Department of Defense (DoD) personnel: Active and reserve (National Guard and Army Reserve) military personnel as well as DoD civilian employees (DoD Instruction 5240.26; DoD, 2012).

Espionage: The act of obtaining, delivering, transmitting, communicating or receiving information in respect to the national defense with an intent or reason to believe that the information could be used to the injury of the United States or to the advantage of any foreign nation and not pursuant to an international agreement duly entered in to by the United States (Army Regulation 381-12).

Information: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, which is owned by, is produced by or for, or is under the control of the U.S. Government (Defense Security Service Regulation 05-06, 2014).

Insider threat: As defined by the Defense Security Service, a threat that an insider will use his/her authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through violent acts, espionage, terrorism, unauthorized disclosure of national security information, or through the loss, denial or degradation of departmental resources or capabilities (Defense Security Service Regulation 05-06, 2014).

Insider: Any person with authorized access to any U.S. Government resource, to include personnel, facilities, information, equipment, networks, or systems (Defense Security Service Regulation 05-06, 2014).

Security education and training: Formal activities, products, and services intended to create or enhance the security knowledge or skills of persons or raise their level of performance, motivation, or operations (DoD Instruction 3305.13, 2014).

Unauthorized disclosure: Communication, confirmation, acknowledgement, or physical transfer of classified information or controlled unclassified information, including the facilitation of, or actual giving, passing, selling, publishing, or in any way making such information available to an unauthorized recipient (Defense Security Service Regulation 05-06, 2014).

Assumptions

The positivist paradigm is based on the belief that knowledge is gained from data that can be directly experienced and verified between independent observers to test a hypothesis through measurement (Goduka, 2012). Although researchers have argued that positivism is based on values of reason, truth, and validity (Blaikie, 1993; Saunders, Lewis, & Thornhill, 2007; Eriksson & Kovalainen, 2008; Easterby-Smith, Thorpe, & Jackson, 2008; Hatch & Cunliffe, 2006), the positivist paradigm involved seeing the world as having a single reality that can be independently observed and measured and where researchers can passively collect and interpret data using tools such as surveys and statistical analysis software (Goduka, 2012). Therefore, aligning positivism with the quantitative research approach permits scientific research through observation and measurement (Goduka, 2012).

Additionally, the meta-theoretical paradigms underlying a quantitative versus qualitative approach was taken into consideration (Gelo, Braakmann, & Benetka, 2008; Lincoln & Guba, 1985; Noblitt & Hare, 1988; Rosenberg, 1988). Quantitative approaches tend to explain phenomena and their relationship to confirm predictions made by a theory, whereas qualitative approaches tend to comprehend personal perspectives, experiences, and understandings of the individual actors (Gelo et al., 2008). Further, qualitative approaches make use of naturalistic designs to study behavior in natural settings (i.e., naturalistic designs; Lincoln & Guba, 1985), but my study was based on a nonexperimental quantitative research approach in which the independent variable cannot be manipulated and the research design will describe the relationship between two or more variables of interest (Gelo et al., 2008).

Scope and Delimitations

The DoD is the largest employer in the world with more than 3 million active, Reserve, and National Guard military members and civilian workforce (DoD, 2016). This study was focused on indicators that identify insider threats and the effectiveness of security education, training, and awareness. To conduct this study, a subset of the population and sample size were selected from the DoD. The subset of the population and sample size will consist of DoD personnel (active, Reserve, and National Guard soldiers, civilians, and contractors) who possess an active security clearance (secret or top secret), that live and work in the United States, and have been employed by the federal government for at least five years.

Furthermore, the dependent variables for this research study were acts of espionage, unauthorized disclosure of information, and any activity resulting in the intentional and unintentional loss of organizational resources and/or capabilities from the actions of an insider. Independent variables were programs designed to mitigate insider threats in which criterion determine whether effectiveness of training, education, and awareness programs changes attitudes, improves knowledge, or increases skills in identifying an insider threat. The control and intervening variables are gender and military and civilian status (e.g., noncommissioned officer, DoD civilian, etc.). The covariates are based on demographics within the DoD. An insider threat can be a male or female, a military member, civilian or contractor. Therefore, analyzing and reporting this data will provide the DoD with information needed to improve current security training, education, and awareness programs among military personnel, government civilians and contractors with access to DoD facilities and organizations (i.e., Army, Air Force, Navy, and Marine Corps)

Sampling Strategy

The use of stratified sampling will address the research questions and hypotheses based on the variables (independent and dependent) for this study. Nonprobability sample designs (convenience, snowball, purposive, and quota samples) were not designed to answer the research questions or hypotheses based on the effectiveness of security education, training, and awareness on identifying insider threats within the DoD.

Moreover, the remaining probability sample designs (simple random, systematic, and cluster sampling) were also not the best choice for selecting sampling size for this study.

Limitations

This study is limited to DoD personnel (i.e., civilians, government contractors, etc.). The DoD is the nation's largest employer with over 3 million employees located all over the world (DoD, 2016). Therefore, the study was limited to the DoD as the source of data collection. This study will include military, civilian, and contractors from all of the military services to ensure validity of the research results. However, there may be biases from senior leadership (military and civilian). These biases will be addressed in the letter to respondents explaining the importance of the study in identifying and reporting insider threats based on current security education, training, and awareness programs.

The final limitation is the amount of time needed by respondents to complete the survey. Personnel needed an adequate amount of time at work to complete the survey. The 10-question survey should take 30 minutes to complete and submit. The survey consisted of closed-ended questions based on demographics (i.e., military rank, branch of service, civilian grade, etc.) and assessed perceptions of DoD personnel on whether current insider threat training is effective.

Significance

The effects of security education, training, and awareness programs on an employees' capability to identify and report insider threats is important to the community and society because the DoD is the United States' first line of defense against all foreign and domestic enemies. After 13 years of war, protecting national security has increased U.S. citizens' trust and dependence on the nation's all volunteer force to provide a safe haven against terrorism. However, recent disclosures of classified documents and information by insider threats are a concern, and research (e.g., Government Accountability Office [GAO] reports and CERT) has shown that mandatory security training, education, and awareness programs are necessary to prevent insider threats. Because the DoD has not developed a specific program or system to identify insider threats, it is important for the DoD to improve its current mandatory training programs and develop a database to identify and track characteristics of insider threats.

This research addresses gaps in the literature on the effectives of security education, training, and awareness programs when identifying and reporting insider threats and provides the DoD with important resources regarding oversight of a very sensitive issue. The DoD has a mission to protect national security from enemies foreign and domestic. Protecting classified information and documents from being compromised by insider threats within the DoD protects U.S. citizens from terrorist attacks in the U.S. and abroad. Since the terrorist attacks on September 11, 2001 and the Boston Marathon in 2013, U.S. citizens live in a world of uncertainty. Therefore, DoD's security education, training, and awareness programs play an important role in ensuring U.S. citizens live and work in a safe and secure environment. This research will assist the DoD with development and implementation of security education, training, and awareness programs as well as a database for tracking potential insider threats.

Summary

This quantitative study was focused on the perceived effectiveness of security education, training and awareness of insider threats within the DoD. Reports from the GAO and DoD regulations and policies, as well as journals and articles, have recognized the need to identify insider threats and improve security education, training, and awareness programs. Leaking information to weaken national security makes an insider threat dangerous. The DoD must understand how and why insider threats exist and how to stop them from committing acts of espionage, which necessitated this study to help understand the effectiveness of security education, training, and awareness programs of insider threats that can help prevent insider threats within the DoD.

Chapter 2 will focus on the literature review based on DoD regulations and articles on the importance of mitigating and addressing insider threats within the DoD. The chapter is also focused on the theoretical frameworks for the study: IAD and the theory of organizational culture and change structure Furthermore, Chapter 2 provides additional literature and research-based analysis on insider threats and the importance of mitigating insider threats based on security education, training and awareness programs, protecting classified information systems, antiterrorism/force protection, cybersecurity, information security, counterintelligence, and policy and strategic initiatives.

Chapter 2: Literature Review

Introduction

After several recent insider threat attacks within the DoD, there is a need to improve security education, training, and awareness programs. The purpose of this quantitative study was to understand the effectiveness of these current programs provided to military, civilian, and government contractors with access to DoD resources, organizations, and facilities. Programs such as the Threat Awareness and Reporting Program (TARP) and DoD mandatory online training courses (i.e., security education training awareness, and antiterrorism/force protection training; see Table 1) are designed to inform and identify types of behaviors of potential insider threats and are required to be completed prior to the end of the fiscal year (October 1–September 30). TARP training is presented by a qualified counterintelligence agent and covers a variety of topics ranging from espionage to insider threats.

Table 1

Elements of Department of Defense Training Programs

	Frequency of Training	Acts of Espionage	Unauthorized Disclosure	Intentional/Unintentional Loss of Organizational Resources
TARP	Annual	Yes	Yes	Yes
SETA	Varies	Yes	Yes	Yes
OPSEC	Annual	Yes	Yes	Yes
AT/FP	Annual	Yes	Yes	Yes

Note. SETA = Security Education Training Awareness, AT/FP = Antiterrorism/Force Protection, OPSEC = Operations Security

Chapter 2 will cover the research literature search strategy, theoretical foundation, and literature review of peer-reviewed articles, DoD regulations and policies, and U.S.

government policies and statues based on insider threats. The literature search strategy involved the use of keywords relevant to the insider threats within the DoD. The theoretical foundation describes how the IAD and theory of organizational culture and change best suits the research study of insider threats. Finally, the literature review will shed light on the published articles related to the research study of insider threats.

Literature Search Strategy

The literature search strategy involved the use of keywords and search engines from U.S. government and military databases. Research articles and peer-reviewed military related journals were obtained from Walden University library's U.S. government and military databases and Google Scholar using the following keywords: *insider threats, Department of Defense, behavior, mitigation, oversight, security, training*, and *education*. Although the Walden University library has several peer-reviewed databases, the military databases were best suited for this research. The following military databases were used: Military and Government Collection and the Homeland Security Digital Library. Searching both databases using the keywords resulted in obtaining the articles used in this research study. Additionally, Zotoro was used to organize articles based on the keywords used in the literature search strategy, which aligned with American Psychological Association guidelines.

Although there is little research about insider threats within the DoD, the articles found in the search provided valuable information about the importance of mitigating insider threats within the DoD. Furthermore, literature used in this study was gleaned from GAO reports, which conducted several investigations into insider threat incidents.

Incidents such as the shootings at Fort Hood, Texas and the Washington Naval Yard involved individuals who had access to classified information and systems and an intent to harm national security. Additional documentation was obtained in the search such as a presidential executive order and memorandum and articles from *National Defense* and *Federal Times* journals as well as U.S. government policies and laws and DoD policies and regulations. The research database results provided literature and resources as far back as 1999. The most recent literature was written in 2017 and provides an in-depth explanation of current insider threats and the training designed to identify them.

Theoretical Foundation

The IAD and the theory of organizational culture and change are the theoretical frameworks that best suit this research study. The IAD draws out assumptions about rules ranging from highly visible statutes to patterns of behavior (Sabatier & Weible, 2014). The theory of organizational culture and change organizational behaviors and decisions are predetermined by assumptions of members within an organization (Shafritz et al., 2016).

Institutional Analysis Development

In 1971, Vincent and Elinor Ostrom developed the IAD to study institutional arrangements. The Ostroms wanted to understand how diverse paradigms in political science affect the way scholars conceptualized public administration and metropolitan organization (Sabatier & Weible, 2014). The IAD framework consisted of four building blocks modeled after the individual, the world of events, decision-making arrangements, and evaluative criteria applied to outcomes (Sabatier & Weible, 2014). Additionally, the

IAD framework was based on the efforts of scholars who wanted to engage and understand problem solving. These scholars were in a quest to devise institutional arrangements in how people solve collective action problems and how to apply it as a means to share problems that people were attempting to resolve.

The IAD is incorporated in DoD's preparation to conduct military operations by focusing on joint military intelligence and civil considerations (Whitfield, 2012). Military leaders use a variety of scholarly disciplines, such as anthropology, sociology, psychology, economics, and political science, when deciding how to decisively conduct military operations. Likewise, the human dimension is a part of the military's operational environment and is composed of multiple fluctuating variables such as individuals, groups, organizations, culture, history, and terrain. These considerations are incorporated into the military's intelligence preparation of the battlefield, which gives them an advantage. Thus, the DoD can take the same approach when addressing insider threats.

The DoD's approach is based on which definition best describes an insider threat. Leaders must not only understand the definition, but they must be able to identify the behavior and ideology of an insider threat. The Joint Publication 3-24 (2017) indicates that an insider threat is a nontraditional threat that undermines counterinsurgency operations, whereas the U.S. Army military intelligence community defines an insider threat as

> A person with placement and access who intentionally causes loss or degradation of resources or capabilities or compromises the ability of an organization to accomplish its mission through espionage, providing support to international

> terrorism, or the unauthorized release or disclosure of information about the plans and intention of the U.S. military forces. (Army Regulation 381-12, 2010)

Further, the DoD must consider an insider threat as the enemy within their organization. Not only are insider threats the enemy, but they are homegrown terrorist not necessarily tied to an organized terrorist effort (Baker, 2012). Although intelligence operations have changed since the Cold War, there has also been a shift to nonstate actors and asymmetric threat tactics following September 11, 2001. To identify and report insider threats, military leaders should incorporate cultural intelligence into doctrinal procedures that are used to conduct intelligence preparation of the operational environment (Whitfield, 2012). The IAD framework facilitates an understanding of the human domain by integrating social science concepts, which can help DoD leadership formulate policy decisions (Whitfield, 2012). The framework can impact how DoD leadership approaches its decision making when it relates to the effectiveness of security education, training, and awareness programs to prevent insider threats.

Organizational Culture and Change

Organizational culture exists within an organization and is composed of many intangible phenomena such as values, beliefs, assumptions, perceptions, behavioral norms, artifacts, and patterns of behavior (Shafritz et al., 2016). The literature on organizational culture has had a dominant theme since the 1980s and tends to reflect unwanted values, such as hierarchy, rigidity, homogeneity, power based on authority, and associations in closed networks. Organizational culture and change are reliant on rules that restrict flexibility and can be barriers to effecting lasting change. In other words, organizational members want to hold on to familiar beliefs, values, policies and practices that they belief serve the organization well. However, it is important for these "command and control" cultures to understand the importance in making changes that encourage and support employee participation and empowerment as well as a more diverse workforce.

Despite the research on organization culture, senior military leaders may not understand the complex task of implementing organizational culture and change within the DoD, which needs both leadership and management (Kelly, 2008). Annual threat assessments like the one presented by former U.S. Army Lieutenant General Michael Flynn have reported how trusted insiders' intent to do harm by exploiting their access to compromise vast amounts of sensitive and classified information were based on personal ideology or at the direction of a foreign government (Flynn, 2014). However, the "command and control" culture can lead to not addressing potential threats such as not discharging Nidal Hasan from the Army despite reports of radical behavior at his previous duty station (Baker, 2012). Although change is difficult, leaders can create a plan to work diligently in shaping the environment and the organizational culture and change to effect a change (Kelly, 2008). For example, for the Joint Fires Observer to succeed, the U.S. Army and U.S. Air Force signed a memorandum of agreement that outlined an understanding of how each organization would operate and coexist within the Joint Fires Observer despite each other's differences in command climate and culture. Leading from the authority of their position and providing follow-up assessments and guidance can ensure that change is a success, which is important to addressing insider threats within the DoD because military and civilian leaders are responsible for the successful implementation of security education, training, and awareness programs.

Literature and Research Based Analysis

Executive Order 13587, which was created to address insider threats, recognized the DoD in conjunction with the National Security Agency as the lead executive agents for safeguarding classified information on computer networks as well as establishing an Insider Threat Task Force co-chaired by the Attorney General and the Director of National Intelligence, or their designees. However, according to a GAO report, the DoD had only complied with the minimum standards outlined in Executive Order 13587 (Kirschbaum, 2015). Although the DoD's culture accepts the fact that changes must be implemented to address insider threats, military leadership is slow to make changes because of the organizational culture of the DoD. Therefore, the IAD and organizational culture and change are the best theoretical frameworks for this study on the effectiveness of security education, training, and security awareness programs on mitigating insider threats because DoD must change their organizational culture to prevent insider threats. These theoretical frameworks have strategic implications for military leaders and scholars and can ensure through security education, training, and awareness programs that personnel (i.e., military, civilian, etc.) recognize and report insider threats based on current policies and laws. Applying multiple echelon approach and scenario-based approaches (i.e., modeling software, etc.) can mitigate insider threats (Baker, 2012). Although insider threats are a high risk to national security, the DoD must work as one organization to address them.

Literature Review Related to Key Variables and Concepts

Espionage

DoD training involves threat awareness programs developed to inform and train soldier, civilians, and contractors against espionage and insider threat (Baker, 2012). Army Regulation 381-12 (2016), TARP, defines espionage as

> The act of obtaining, delivering, transmitting, communicating or receiving information in respect to the national defense with an intent or reason to believe that the information could be used to the injury of the United States or to the advantage of any Foreign Nation and not pursuant to an international agreement duly entered into by the United States.

Committing espionage against the United States is a crime in which service members are charged under the Uniform Code of Military Justice 906a. Article 106a. Spies/Espionage. According to Article 106a., no person may be sentenced by court-martial to suffer death for an offense under this article unless the member of the court-martial finds at least one of the aggravating factors set out in subsection (c), and the members unanimously determine that the aggravating circumstances or factors outweigh other circumstances. Subsection (c) states that a sentence of death may be given only if the members unanimously find, beyond a reasonable doubt, one or more of the following aggravating factors: being convicted of another offense involving espionage or treason for which either a sentence of death or imprisonment for life was authorized by statute, knowingly creating a grave risk of substantial damage to the national security or risk of death to another person, and any other factor that may be prescribed by the president by regulations under section 836 of this title (Article 36).

The Defense Personnel and Security Research Center (PERSEREC) was created in 1986 to perform behavioral science research on personnel security policies and practices after John Walker, a U.S. Navy cryptographic radioman, committed espionage in 1985. Furthermore, to improve security education and awareness, PERSEREC published unclassified analytical reports about espionage for public distribution. In PERSEREC's fourth series of unclassified analytical reports on espionage, Herbig (2017) compared data across three cohorts of persons based on the time period they committed espionage. The three cohorts are as follows: 1947–1979 (Early Cold War), 1980-1989 (Later Cold War), and 1990-2015 (post-Soviet period). Since 1990, three-quarters of espionage-related offenses have been committed by civil servants and one-quarter military personnel as compared to the previous two cohorts where an increased proportion were contractors or have held jobs not related to espionage or have not held security clearances (Herbig, 2017).

For decades, insiders with privileged access to classified or sensitive information betrayed the U.S. by committing espionage. In 2013 and 2015, there were two cases of espionage and unauthorized disclosure of information by insiders within the DoD (Lamothe, 2016). In 2013, an Army military police officer, Specialist William Colton Millay, was sentenced to 16 years of confinement for trying to sell military secrets to an FBI agent (Thiessen, 2013). In 2015, Navy Lieutenant Commander Edward Lin was secretly arrested in Kaneohe Bay, Hawaii by the Naval Criminal Investigative Service for communicating secret information with intent or reason to believe it would be used to the advantage of a foreign nation and other charges. The Naval Criminal Investigative Service and the FBI were investigating whether Lieutenant Commander Lin passed classified information to both China and Taiwan (Lamothe, 2016; Larter, 2017). As of May 4, 2017, Lin pled guilty of communicating national defense information under the Federal Espionage Act as well as guilty to offenses of orders violations and making false official statements under the Uniform Code of Military Justice. On June 2, 2017, Lin was sentenced to 6 years in prison (WFMY, 2017).

Another case of an insider threat was in 2010, when Army Specialist Bradley Manning was arrested while deployed to Iraq and detained in Kuwait after providing unauthorized disclosure of classified information to Wiki Leaks (Tate, 2010). During his court-martial, Manning was demoted to Private First Class and detained in the Quantico Confinement Facility at Marine Corps Base Quantico, Virginia. Manning was sentenced to 35 years and dishonorably discharged from the military in 2013 (Martinez & Saenz, 2013; Tate, 2013). Although Manning was sentenced to 35 years at the U.S. Disciplinary Barracks at Fort Leavenworth, Kansas, he only served seven years of his sentence. President Barack H. Obama commuted his sentence in 2017 (Savage, 2017). Manning was released from U.S. Disciplinary Barracks May 17, 2017 (Onyanga-Omara & Vanden Brook, 2017).

Further, leaks by Manning in 2010 and Snowden in 2013 are quite common (Herbig, 2017). For example, between 2005 and 2009, 153 suspected cases were referred to the Department of Justice. However, the Department of Justice opened only 26 cases and identified 14 suspects, none of which led to an indictment (Harris, 2010; LaFraniere, 2013).

Unauthorized Disclosure

Unauthorized disclosure is a communication or physical transfer of classified information or controlled unclassified information to an unauthorized recipient (Center for Development of Security Excellence, 2017). Unauthorized disclosure can occur intentionally or accidentally through leaks, data spills, espionage, or not following proper safeguarding procedures.

Leaks are deliberate disclosures of information to the media. Examples of leaks are information about top secret government surveillance programs to news outlets and Manning's intentional leak of thousands of classified documents to WikiLeaks.

Data spills are willful, negligent, or inadvertent disclosures of classified information or controlled unclassified information across computer systems. For example, opening information from the Secured Internet Protocol Router Network on the Nonsecured Internet Protocol Router Network) can create the potential for rapid and widespread unauthorized disclosure causing a data spill or negligent discharge of classified information. Data spills (negligent discharges of classified information) are considered a possible compromise of classified information. The most common data spills (negligent discharges of classified information) are through an email or publicly accessible internet sites.

Unauthorized disclosure due to improper safeguarding procedures is usually unintentional but can be just as damaging to national security as leaks, data spills, and espionage. Examples of improper safeguarding procedures is leaving a classified document on a photocopier, forgetting to security classified documents before leaving the office, discussing classified information within an earshot of unauthorized recipients, and dual-use technology (used for military and commercial use).

According the Gaston (2017), damage caused by unauthorized disclosures is based on the following three levels of classification: confidential, secret, and top secret. Confidential is the lowest level of classification in which unauthorized disclosure can cause "damage" to national security. Unauthorized exposure of secret information can cause "grave damage" to national security while "exceptionally grave damage" to national security is caused by unauthorized exposure of top-secret information. Each level of classification is designed to compartmentalize information to allow only persons cleared at the appropriate level access to information (Young, 2017).

On September 8, 2017, the White House issued the following guidance: "Unauthorized disclosure of classified information or controlled unclassified U.S. Government information causes harm to our nation and shakes the confidence of the American people." Accordingly, the Secretary of Defense (SECDEF) published Executive Order (EXORD) 009-18, DoD Training on Unauthorized Disclosure, on September 19, 2017. EXORD 009-18 directed every DoD department and agency to dedicate one hour, during the month of October 2017, to engage their organization in discussion on the importance of protecting classified and controlled unclassified information and measures to prevent and detect unauthorized disclosures.

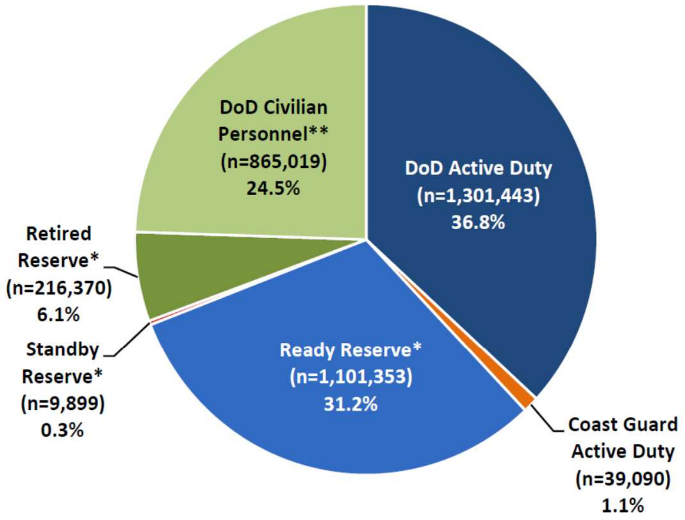
Unauthorized disclosure of information harms the U.S. through damage to national security and loss of life, money, public trust and confidence and a way of life. It also undermines ongoing and planned military operations, damages intelligence methods and sources, impacts our international alliances and foreign policy and benefits adversaries wishing to harm the U.S.

Those involved in unauthorized disclosure may face serious consequences. After the investigation is conducted, military commanders and supervisors may consider and impose a wide range of sanctions and actions against those responsible for unauthorized disclosure of classified information. These consequences can take the form of Uniform Code of Military Justice sanctions, civil litigation, and administrative and/or criminal sanctions. Many of these sanctions were imposed on Bradley Manning for his unauthorized disclosure to WikiLeaks.

Intentional and Unintentional Insider Threats

Threats may be intentional or unintentional and can come from internal and external sources (Yaokumuh & Kumuh, 2018). According to the CERT Insider Threat Team, both intentional and unintentional insider threats are characterized based on the sociological context of trust, workplace behaviors, and fallibility (CERT, 2013). Intentional insider threats tend to originate from malicious intentions and seek to harm an organization's information assets. Furthermore, intentional insider threats are more dangerous because they deliberately access information in an unauthorized manner and are usually technically capable of using social engineering techniques along with sophisticated technical expertise to gain unauthorized access to an organization's valuable resources (Omar, 2015). On the other hand, an unintentional insider threat lacks the understanding of security policy and does not conform to security awareness and training programs (Omar, 2015). However, enforcing clear security policies and guidelines are effective ways to mitigate intentional and unintentional insider threats within an organization.

For example, U.S. Government nuclear facilities are improving insider threat training, awareness programs, and mitigation by using tabletop exercises developed by Sandia National Laboratories (Abbott, 2017). One of the tabletop exercises uses a case study to highlight intentional and unintentional insider threats (Abbott, 2017).



* Includes Coast Guard Reserve

** Includes Non-Appropriated Funds civilians and Appropriated Funds civilians

Note: Percentages may not total to 100 due to rounding.

Source: Official Guard and Reserve Manpower Strengths & Statistics FY 2015 Summary

Figure 1. 2015 military personnel and DoD civilians demographics report. This pie chart presents all branches of the military (active duty, Reserve and National Guard) and the Department of Homeland Security Coast Guard, as well as DoD civilian personnel who support the DoD, DoD Office of the Deputy Assistant Secretary of Defense for Military Community and Family Policy (2015).

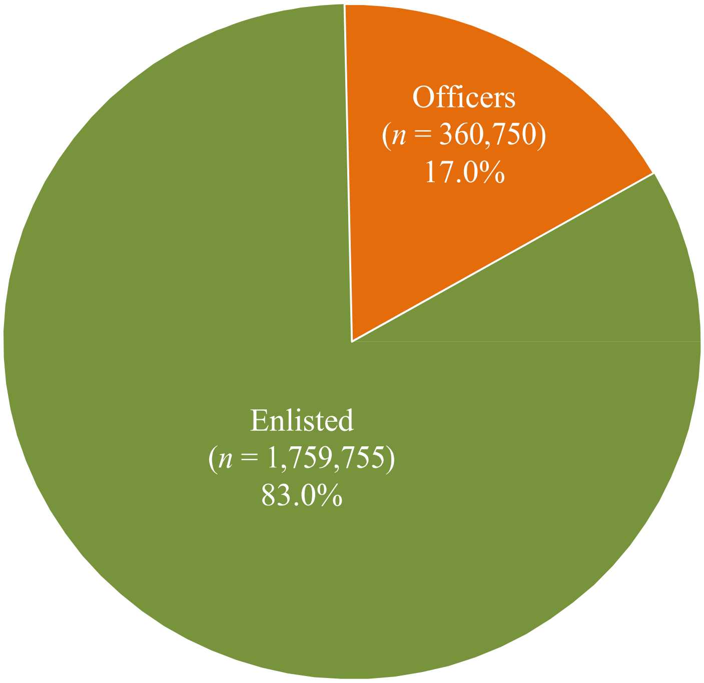


Figure 2. Enlisted members and officers in the total military force.

This pie chart represents the total number of active duty and selected Reserve enlisted members (noncommission officers [NCOs]/petty officers [POs]) and officers (commissioned and warrant officers) across the DOD. Overall, the total DoD force is composed of 1,759,755 (83%) enlisted members and 360,750 (17%) officers, Defense Manpower Data Center (DMDC), 2015. Note that the percentages may not total to 100 due to rounding. Source: DMDC Active Duty Military Personnel Master File (September 2015); DMDC Reserve Components Common Personnel Data System (September 2015)

The DoD employs over 3 million individuals all over the world. Figures 1 and 2 above depict the graphical analysis of the demographics for the 3 million military and

DoD civilians. Whereas Figures 3 and 4 below depict the graphical analysis of both appropriated and nonappropriated DoD civilian employees. The data and support for the graphical analysis was provided by the DMDC and published in the Office of the Deputy Assistant Secretary of Defense for Military Community and Family Policy 2015 report.

Officer

The DoD officer ranks consider of commissioned officers and warrant officers. The commissioned ranks are the highest in the military. Military officers hold presidential commissions and their ranks are confirmed by the U.S. Senate. Army, Air Force and Marine Corps officers are called company grade officers in the pay grades of O-1 to O-3, field grade officers in the pay grades of O-4 to O-6 and general officers in pay grades O-7 and higher. The Navy's equivalent officer groupings are called junior grade, mid-grade and flag.

Warrant officers are specialists and experts in certain military occupational specialties and hold warrants from their service secretary. The lowest ranking warrant officers serve under a warrant, but they receive commissions from the president upon promotion to chief warrant officer 2. Although warrant officers derive their authority from the same source as commissioned officers, they remain specialists in contrast to commissioned officers who are generalists. There are no warrant officers in the Air Force.

Enlisted

Enlisted service members in the pay grades of E-1 through E-4 are usually either in training status or on their initial assignment. According to Enlisted Leaders (2013), training includes the basic training phase where recruits are immersed in military culture and values and are taught the core skills required by their service component (i.e. Army, Air Force, Navy, and Marine Corps). After completing basic training, recruits begin specialized or advanced training which provides them with a specific area of expertise or concentration. In the Army and Marine Corps, this area is called a military occupational specialty; in the Navy it is known as a rate; and in the Air Force it is simply called an Air Force specialty (Enlisted Leaders, 2013).

Noncommissioned Officer/Petty Officer

Enlisted members in the Armed Forces are members of the Profession of Arms and have taken an oath of enlistment to support and defend the Constitution. The NCO/ PO is known as "the backbone" of the Armed Forces and are empowered and trusted to lead today's all-volunteer force. NCOs/POs are leaders and technical experts who enhance organizational effectiveness and directly contribute to mission success. NCOs/POs are responsible and accountable for the development and welfare of their subordinates. They teach, coach and mentor them as well as enforce military standards. NCO/PO pay grades are E-4 (Corporal) through E-9.

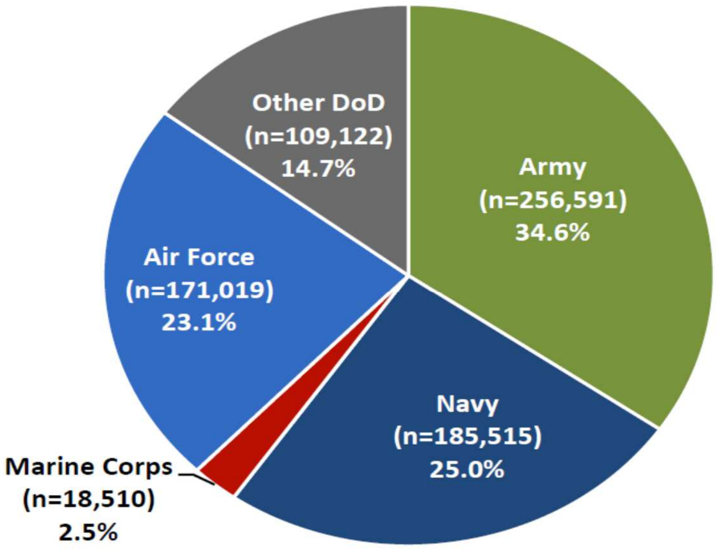


Figure 3. DoD appropriated funds civilians. This pie chart represents the distribution of APF civilian personnel working for the DoD. There are 740,757 (21%) APF civilian personnel in the total DoD workforce. The largest percentage are employed by the Army (34.6%) while the smallest are employed by the Marine Corps (2.5%), DMDC DoD APF Civilian Master File, 2015

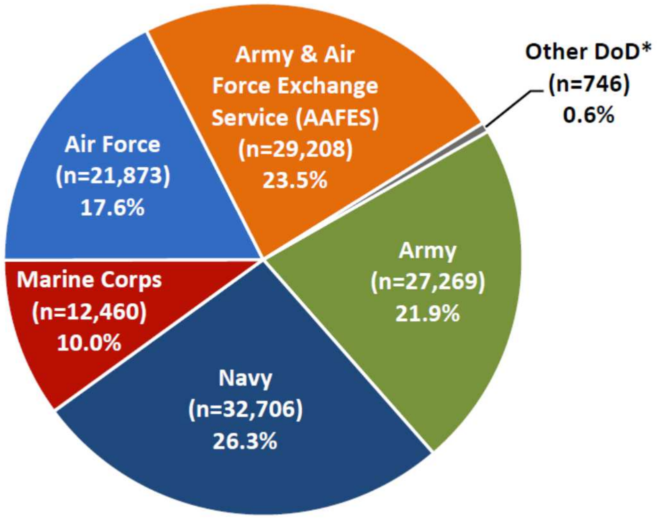


Figure 4. DoD non-appropriated funds civilians. This pie chart represents the distribution of NAF civilian personnel. There are 124.262 (3.5%) NAF DoD civilians in the total DoD workforce. The largest percentage are working for the Navy (26.3%) while the remainder (0.6%) work within other areas of DoD, DMDC DoD NAF civilian file, 2015.

Department of Defense Civilian

DoD civilians are federal employees directly hired and paid from appropriated or nonappropriated funds, under permanent or temporary appointment. Many DoD civilians are former members of the military (i.e. veterans or retirees) while others are hired as interns or due to skills obtained from private sector employment. DoD civilians have three levels of employment: entry level; mid-career level; and executive level.

Entry level employees fill positions typically suited for those graduation from college with little or no work experience. DoD select the best and brightest to be part of the team, by creating a stimulating corporate culture of openness, integrity, and creativity. DoD entry level employees participate in an exceptional environment that provides growth, recognition, and continuous learning. DoD invest in its employees because they want to attract and retain the very best.

Mid-career level employees are creative, team-oriented colleagues who bring intensity and integrity, intellectual curiosity and leadership potential to the team. Most veterans and retirees fall in the mid-career level category. Mid-career employees possess extensive experience and are technically competent in one or more areas. The developmental focus of mid-career level employees is team building, interpersonal skills, and program management.

Executive level employees are executives and managers who lead and motivate people, who are results-driven and achieve those results through partnerships and building coalitions, and who have a keen business sense about using their resources to get the best results possible. Executive level employees are exceptional leaders with the ability to design and implement strategies that maximize employee potential and foster high ethical standards that will enable DoD to serve the American people effectively. Individuals at this level are developed through broad-based assignments requiring staff contacts with top management, officials within DoD, outside agencies, and industry.

Overall, DoD employees at all levels benefit from a competitive salary and benefit package, annual salary increases for satisfactory performance, job security, responsibility, challenging work and a valuable retirement plan.

Defense Contractor

DoD relies on the private sector to carry out specific aspects of the department's mission. Critical reliance on contractor support is crucial for the DoD because the federal government wants to receive the best value for the warfighter at the tax payer's expense. Furthermore, the contractor is response for carrying out its obligations under the contract in terms of quality, timeliness, and cost. Although defense contractors are an important component of the total DoD force, they are not federal government employees.

Insider threats pose a threat to national security inside and outside of the United States (U.S.). Although it is often difficult to detect and deter insider threats, the DoD has developed polices mandating security education, training, and awareness programs as a means to mitigate and thwart insider threats. In September 2014, the DoD insider threat policy required each military component (i.e. Army, Air Force, Marine Corps, and Navy) to issue respective policies and plans. As a result, according to the Defense Security Service, a sub-agency of the DoD, an insider threat poses a risk by using his/her access to classified information to do harm to the United States through acts of espionage, terrorism, unauthorized disclosure of national security information (Defense Security Services Regulation 05-06, 2014).

Department of Defense Policies

DoD Directive 5205.16, The DoD Insider Threat Program, August 28, 2017, establishes policy and assigns responsibilities within the DoD to develop and maintain an insider threat program to comply with the requirements and minimum standards to prevent, deter, detect, and mitigate the threat insiders may pose to the DoD and U.S. government installations, facilities, personnel, missions, or resources. The DoD Directive 5205.16 identifies appropriate security training, education, and awareness initiatives that may be made available to DoD personnel (i.e. military and DoD civilians) and defense contractors. DoD Directive 5205.16 policy implements the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs by gathering, integrating, reviewing, assessing and responding to information derived from sources (i.e. security, cybersecurity, counterintelligence, workplace violence, etc.) as necessary and appropriate to identify, mitigate, and counter insider threats (DoD, 2017b).

DoD Instruction 3305.13, *DoD Security Education, Training and Certification*, February 13, 2014, establishes policy, standards, and procedures and assigned responsibilities for conduct of DoD security education, training and professional development. DoD Instruction 3305.13 (2014) ensures DoD develop and maintain security education, training and certification programs that are technically sound and support DoD missions.

DoD Instruction 5205.83, DoD Insider Threat Management and Analysis Center (DITMAC), March 30, 2017, establishes policy, assigns responsibilities, and prescribes procedures for the DITMAC. The DITMAC serves as the DoD's enterprise-level capability for insider threat information integration, and management by managing and analyzing insider threat information across law enforcement, personnel security, human resources, counterintelligence, physical security, network behavior monitoring, and cybersecurity activities of all military services pursuant to Executive Order 13587. DITMAC policy is in accordance with Executive Order 13587 and DoD Directive 5205.16 by integrating and centrally analyzing key threat-related information that insider threats pose to DoD and U.S. government installations, facilities, personnel, missions, or resources (DoD Instruction 5205.83, 2017). This includes damage to the U.S. through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities (DoD Instruction 5205.83, 2017).

DoD Manual 3115.11, DoD Intelligence and Security Training Standards, revised on September 8, 2016, provides validated learning requirements to the DoD intelligence and security communities learning functions. DoD's intelligence and security training management functions validate learning requirements by participating in gap analysis, coordinating with DoD functional managers and their respective training councils, and validating learning requirements. After the requirements are validated, the intelligence and security training management functions translate requirements into action plans, coordinate with existing learning assets to identify shared resources and services and allocate resources to develop learning solutions. Additionally, the DoD intelligence and security training functions support the development and delivery of learning to intelligence and security schoolhouses and DoD component training assets.

Security Education, Training, and Awareness Programs

Mandatory security education, training, and awareness programs are key to mitigating and thwarting insider threats and provides a means to reinforce the need for heightened security awareness (DoD, 1999). Therefore, DoD must establish security/counterintelligence related education and training awareness programs to prevent incidents like the shootings at Fort Hood, Texas and the Washington Naval Yard. Additionally, security education, training, and awareness programs should primarily focus on identifying and reporting "insiders" possessing characteristics based on the definition of an insider threat.

DoD Directive 5205.16, The DoD Insider Threat Program designates the Defense Security Service as the office for providing insider threat security education, training, and awareness programs to DoD components (i.e. Army, Air Force, Marine Corps, and Navy) and vetted DoD contractors (DoD, 2017b). DoD component heads are responsible for incorporating annual insider threat security education, training and awareness programs in accordance with DoD Directive 5240.06, Counterintelligence Awareness and Reporting, (DoD, 2017a) and DoD Directive 5240.02, Counterintelligence (DoD, 2015b).

Kim & Homan (2012) measured the effectiveness of information security training by comparing CBT and IBT. The study asked 212 Federal government employees to choose either CBT or IBT. A pre-test knowledge quiz was administered prior to the training sessions. After the training sessions were complete, a 60-day and 90-day post-test knowledge quiz was completed by participants. The pre-test and post-test results of this study implied that an organization must repeatedly provide reminders of training materials in order for training to have a lasting effect. Although CBT programs are becoming more common in government and private organizations, the results of Kim & Homan's (2012) study showed that IBT programs are just as effective as CBT programs in raising the level of security awareness. Therefore, the DoD's use of both CBT and IBT programs are very effective in providing insider threat security education, training and awareness programs.

In addition to security education, training and awareness programs, the U.S. Army's Asymmetric Warfare Group based at Fort Meade, Maryland developed an insider threat model intended for U.S. Army personnel to act and report suspicious terrorist threats (Baker, 2012). The model divides the observables indicators into three categories and attempts to differentiate between the high-risk individual and the terrorist insider threat individual as seen in Table 2.

OBSERVABLE INDICATORS

Category I Indicators

- Complains about other nations or religions
- Advocates violence beyond what is the accepted norm
- Abrupt behavioral shift
- Desires control
- Socially withdraws in some occasions
- Appears frustrated with partnered nations
- Experiences personal crisis
- Demonizes others
- Lacks positive identity with unit or country
- Reclusive
- Strange Habits
- Peculiar Discussions

Category II Indicators

- Verbally defends radical groups and/or ideologies
- Speaks about seeking revenge
- Associates with person that have extremist beliefs
- Exhibits intolerance
- Personally connected to a grievance
- Cuts ties with unit, family, or friends
- Isolates self from unit members
- Intense ideological rhetoric
- Attempts to recruit others
- Choice of questionable reading material sin personal areas

Category III Indicators

- Advocates violence as a solution to problems
- Shows a sudden shift from "upset" to normal
- Takes suspicious travel or unauthorized absences
- Stores or collects ammunition or other items that could be used to injure or kill multiple personnel
- Verbal hatred of partner nation or individual from partner nation
- Exhibits sudden interest in partner nation headquarters or individual living quarters
- Makes threatening gestures or verbal threats

Figure 5. Asymmetric warfare group observable indicators of insider threats. This model has 29 observables and appears more extensive than any other model better allowing for prevention of insider threat. From "Insider Threats in Partnering Environments, A Guide for Military Leaders", by Asymmetric Warfare Group, 2011.

Protecting Classified Information and Systems

Recent disclosures of classified information and documents by insider threats have been disconcerting for the DoD. As a result, Defense Security Service established an insider threat identification and mitigation policy and procedures to identify, deter and detect insiders who pose a risk to operations or classified information and systems (Defense Security Services Regulation, 2014).

Presidential Executive Order 13587 directed all government agencies to include six minimum standards into their insider threat programs. Executive Order 13587 also directed reforms on how DoD personnel (military, civilians, and contractors) share and safeguard classified information on computer networks. Although Executive Order 13587 was enacted to improve the security of classified information, it also included a provision to prohibit its use for identifying or preventing whistleblowers from making lawful disclosures.

On January 6, 2016, 22 human and civil rights, whistleblower protection and advocacy, lobbying, and free speech and freedom of the press organizations wrote a letter to the Inspector General of the Intelligence Community, Charles McCullough, III, explaining the important role that whistleblowers play in the proper functioning of the federal government. The letter revealed how internal training conducted by the Office of the Director of National Intelligence mischaracterized whistleblower Thomas Drake as an "insider threat' placing him in the same category as Nidal Hasan and Aaron Alexis.

According to the Government Accountability Project, Thomas Drake experienced retaliation and reprisal after reporting a mass amount of waste and abuse in the billions of dollars spent on Operation Steller Wind to his superiors at the National Security Agency, Congress and the DoD Inspector General. In April 2010, the Department of Justice indicted Drake under the Espionage Act of 1917 with improper retention of allegedly classified information. Department of Justice charged Drake under 10 separate counts, but he only faced five charges under the Espionage Act of 1917. Eventually, Department of Justice's case against Drake collapsed and the Department of Justice dropped the tencount felony indictment including the espionage charges. Drake pled guilty to a misdemeanor, "exceeding authorized use of a computer" and was sentenced to one year of probation and community service thanks to the efforts of the media and Government Accountability Project. Unfortunately, this is not the first time Office of the Director of National Intelligence erroneously mischaracterized insider threats and whistleblowers. Therefore, government agencies must understand that section 7(e) of Executive Order 13587 directs government agencies not to seek to deter, detect, or mitigate disclosures of information by government employees or contractors that are lawful under and protected by the Intelligence Community Whistleblower Protection Act of 1998, Whistleblower Protection Act of 1989, Inspector General Act of 1978, or similar statutes, regulations, or policies (Obama, 2011).

Executive Order 13587 has been supported and criticized by Congressional lawmakers as well as the general public. Several Congressional lawmakers supported Executive Order 13587 as another weapon against cyber-attacks, while others say it will not solve America's cyber problems (Harmon, 2015). For example, California Representative Adam Schiff praised President Obama's efforts to secure public and private networks from cyber-attacks and espionage, while Speaker of the House John Boehner urged President Obama to work with Republicans in Congress to create an information-sharing bill instead of imposing an Executive Order

The DoD structured its insider threat program to address insider threats based on Executive Order 13587. As a result, DoD's program includes four broad types of insider threats: Antiterrorism/Force Protection, Cybersecurity, Information Security, and Counter Intelligence. (Kirschbaum, 2015).

Antiterrorism/Force Protection

The incidents at Fort Hood, Texas in 2009 and the Washington Navy Yard in 2013 forced DoD to review its Antiterrorism/Force Protection efforts when addressing insider threats (Kirschbaum, 2015). The U.S. Army's online annual Antiterrorism/Force Protection training (i.e. Army Regulation 381-12, Military Intelligence TARP) and curriculum on the Joint Knowledge Online website recommended a process to identify insider threats based on high-risk behaviors and level of threat activity (Baker, 2012).

It is important for personnel to participate in threat awareness training and education because the DoD is a prime target for exploitation by foreign intelligence and international terrorist organizations and from insider threats. Protecting the lives of troops depends on knowledge, awareness, and participation in threat awareness and reporting. It is essential to increase security education, training, and awareness programs in order to inform insiders of their responsibilities, to reduce carelessness and to inform the potential insider threat of the consequences of such behavior (DoD, 1999). Therefore, security education, training, and awareness programs play an important role in protecting the lives of troops as well as protecting national security at home and abroad. For example, Army Regulation 381-12 states that all Department of the Army personnel will receive TARP training within 30 days of assignment or employment to an organization followed by mandatory annual TARP training in a live environment conducted by a qualified counterintelligence agent. Department of the Army defined a qualified counterintelligence agent as those who have successfully completed the TARP T3 program (Army Regulation, 381-12, 2016). TARP formerly known as Subversion and Espionage Directed Against the United States, establishes policy and responsibilities for threat awareness and reporting in the U.S. Army.

Army Regulation 381-12, TARP, outlines the U.S. Army's primary method of educating the force about insider threats. Army Regulation 381-12 provides policy and responsibilities for threat awareness and education and establishes a requirement for Department of the Army personnel to report any incident of known or suspected espionage, international terrorism, sabotage, subversion, theft or diversion of military technology, information systems intrusions, and unauthorized disclosure of classified information (Deming, 2017). Military personnel who fail to report insider threats are subject to punishment under Uniform Code of Military Justice as well as to adverse administrative or other adverse action authorized by provisions of the U.S. Code or Federal Regulations. Civilian personnel and contractors are subject to adverse administrative actions or criminal prosecution as authorized by applicable provisions of U.S. Code or Federal Regulations. Failure to educate personnel to report insider threats leads to loss of life as in the cases of Army Sergeant William Kreutzer, Jr. at Fort Bragg, North Carolina.

Sergeant Kreutzer exhibited signs of extreme behavior in which he wanted to kill fellow soldiers for teasing and disrespecting him. Sergeant Kreutzer's mental health continued to deteriorate due to personal and professional issues. He was teased and called nicknames by fellow soldiers which frustrated him to the point where he wanted to shoot and kill members of his team. Unfortunately, on October 27, 1995 Sergeant Kreutzer armed with two semi-automatic rifles, two pistols, a knife, and nearly 900 rounds of ammunition methodically wounded eight soldiers and killed one while 2nd Brigade, 82nd Airborne Division prepared for a brigade run (Deming, 2017). This attack by an insider threat was preventable, but fellow soldiers failed to report Kreutzer's behavior to leadership and leaders failed to acknowledge him as a threat and discharge him from military service.

Cybersecurity

In 2015, the GAO released a report on widespread cybersecurity weaknesses at most federal agencies making DoD uniquely susceptible to cybersecurity data breeches (Rotenberg, Gartland, Lipsitz, & Moscardini, 2016). Federal agency computer systems face an evolving array of cyber-based threats that are unintentional and intentional. Unintentional threats range from software coding errors to the actions of careless or poorly trained employees. Whereas intentional threats are targeted or untargeted attacks from criminals, hackers, adversarial nations, terrorist, disgruntled employees or other organizational insiders (Willemssen, et. al., 2015). Over the last several years, federal agencies expressed their concerns regarding recent incidents involving breeches of sensitive data. Figure 5 below depicts the sharp increase in information security incidents reported have risen from 5,503 in fiscal year 2006 to 67,168 in fiscal year 2014.

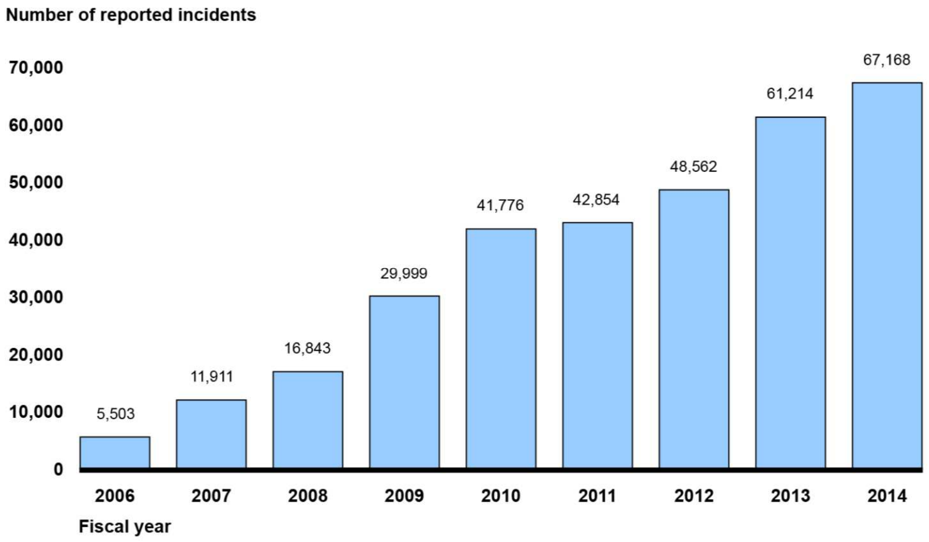


Figure 6. Incidents reported to the U.S. computer emergency readiness team by federal agencies, fiscal years 2006 through 2014.GAO analysis of United States Computer Emergency Readiness Team data for fiscal years 2006-2014, GAO-15-194T, 2015.

In 2016, DoD decided to take a proactive measure by planning to build a database to monitor, analyze and identify insider threats in accordance with Executive Order 13587. DoD's database, officially titled Insider Threat Management and Analysis Center and DoD Component Insider Threat Records System, provides a non-exhaustive list of insider threats including those causing damage to the U.S. through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities (Gartland, Lipsitz, & Moscardini, 2016).

In another research study, cybersecurity expert, Dr. Eric A. Cole, analyzed data based on studies conducted by CERT and the U.S. Secret Service and determined that profiled insiders often displayed warning signs prior to their actions against an organization. According to Cole (2012), 80% of insiders who launched attacks against their organizations had displayed negative behaviors prior to the incident; 92% experienced a negative work-related event (e.g. demotion, transfer, or termination); and 59% were former employees or contractors (Cole, 2012).

Mills, et. al., (2011) scenario-based approach to mitigating insider threats analyzed insider threats in multiple layers starting with personal interactions or observables layered with informational auditing of cyber actions. The scenario-based approach gives the organization the ability to identify its critical information resources by using these resources to work through scenarios to pinpoint possible insider attacks. Using this approach helps the organization develop the necessary adjustment or validations needed for their defense systems (Baker, 2012).

In an effort to mitigate and thwart insider threats, Executive Order 13587 ordered federal agencies to create insider threat detection and prevention programs. Executive Order 13587 also requires federal agencies to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties (Rotenberg, Gartland, Lipsitz, & Moscardini, 2016).

Information Security

Three independent inquiries were commissioned by the DoD, FBI, and U.S. Senate after Army Major Nidal Hasan opened fire at the Soldier Readiness Center at Fort Hood, Texas on November 5, 2009 killing 13 soldiers and injuring 43 (Aradau & Blanke, 2017). The DoD, FBI, and U.S. Senate debated whether or not Hasan’s motives were a case of terrorism, an instance of violent Islamic extremism, or simple workplace violence (Baker, 2012). However, public debate evolved around whether digital technologies and information would have provided better information sharing among the DoD, FBI, and U.S. Senate. While the FBI's inquiry highlighted 'the ever-increasing challenge that electronic communications pose to identify and avert potentially destructive activity', the U.S. Senate inquiry looked for clues the FBI had available buy missed given that it lacked the totality of the information or failed to 'connect the dots'. Unfortunately, in the wake of the Fort Hood, Texas attack the use of the Defense Advanced Research Projects Agency (DARPA) Anomaly Detection at Multiple Scales (ADAMS) software went largely unnoticed. Since the Fort Hood, Texas shooting, anomaly detection software has emerged as a key area of security professionals by showing the promise of Big Data to capture the 'unknown of unknowns' and departing from the digital techniques that concentrate on analyzing known suspects or profiling risky individuals such as Edward Snowden (Aradau & Blanke, 2017).

Accelerating growth of the Internet and development of information technology have brought a rapid increase in the use of open and shared network systems. These network systems improve the ability to provide DoD organizations with access to data and make them vulnerable to service interruptions, theft, or altercation of data (Kim & Homan, 2012). Insider threats exploit information security by exposing radical views using computers and the Internet (Baker, 2012). In order to thwart an insider threat's exploitation of DoD's information systems, other processes must be developed to oversee human monitoring. Therefore, DARPA created a new detection software to assist DoD with mitigating and thwarting an insider threat's exploitation of information systems.

DARPA uses ADAMS software to develop a set of algorithms which detects anomalous behavior before damage is done. ADAMS' software-based approach tracks a person's online work activity in an effort to detect anomalous behavior. In order for the data to be useful in thwarting and mitigating insider threats it must contain detailed accounts of human behavior within a monitored environment. Once the data is collected, ADAMS analyzes it and highlights the potential threats. Using DARPA's ADAMS software-based approach is DoD's best defense against exploitation of insider threats because it protects DoD's information systems from breeches caused by insider threats.

In the months following the WikiLeaks revelations, DARPA put out requests for research on methods to detect suspicious behavior in large datasets to root out rogue actors like Manning and Hasan (Keating, 2013). ADAMS was one of the most ambitious programs meant to create, adapt and apply technology to the problem of anomaly characterization and detection in massive datasets and would develop computers that could analyze a large set of user-generated data

Unfortunately, there is a downside to collecting real data for research using the DARPA's ADAMS software-based approach because of ethical, legal, confidentiality, and privacy concerns. Therefore, proxy data sets and synthetic data were used for the ADAMS software-based approach for research purposes. Glasser & Lindauer's (2013) research generated synthetic data to simulate the aggregated collection of logs from host-based distributed across all computer workstations within a large business or government organization over a 500-day period. Using synthetic data can control and rapidly and economically generate data sets with desired characteristics, size, and quality relative to measurable characteristics. The data sets are fully intact and free of privacy restrictions or limitations (Glasser & Lindauer, 2013).

Counterintelligence

Lone wolf actors are often successful at insider threat attacks. For example, U.S. Army Medical Command leadership failed to reprimand Army Major Nidal Hasan for his actions prior to the 2009 Fort Hood, Texas shooting (Baker, 2012). Hasan's chain of command at the Uniformed Services University of the Health Sciences had identified him, as early as 2007, as unprofessional and possessing radical beliefs. Hasan was also referred to the FBI for possible terrorist activity. Although, the FBI confirmed Hasan's activity, they determined it had been for research purposes for his Master in Public Health degree. Globalization, rapid technological advancements, and uncertain fiscal environment present new avenues of collection and threats from foreign intelligence services and entities that target U.S. national security, information systems, and personnel. Insider threats are often lured to commit acts of espionage by exploiting their access to compromise vast amounts of sensitive and classified information as part of personal ideology or at the direction of foreign intelligence entities. Treacherous acts such as illegally released information by WikiLeaks and Edward Snowden highlight a link between counterintelligence and the need to identify and report insider threats before they cause grave risk to national security and put lives at risk (Committee on Homeland Security House of Representatives One Hundred Fourteenth Congress, 2016). These unauthorized disclosures continue to pose a critical threat to national security (Flynn, 2014).

Counterintelligence operations are also used in criminal investigations due to the goal of seeking out suspects who have committed national security crimes such as espionage, sedition, or terrorism (Stockham, 2017). Therefore, DoD must also ensure each military service law enforcement capabilities are incorporated into its counterintelligence operations.

Although nearly 140 nations and some 35 known suspected terrorist organizations currently target the U.S. for intelligence collection, the number of potential insider threats waiting to strike or steal classified information brings the threats even higher (Stockham, 2017). These insiders work on behalf of foreign adversaries or as lone wolves. When there is a critical risk to national security (i.e. Manning and Snowden), DoD conducts aggressive and comprehensive counterintelligence investigations that are intended to detect, identify, exploit, and neutralize the foreign intelligence entities and insider threat to the DoD (Stockham, 2017).

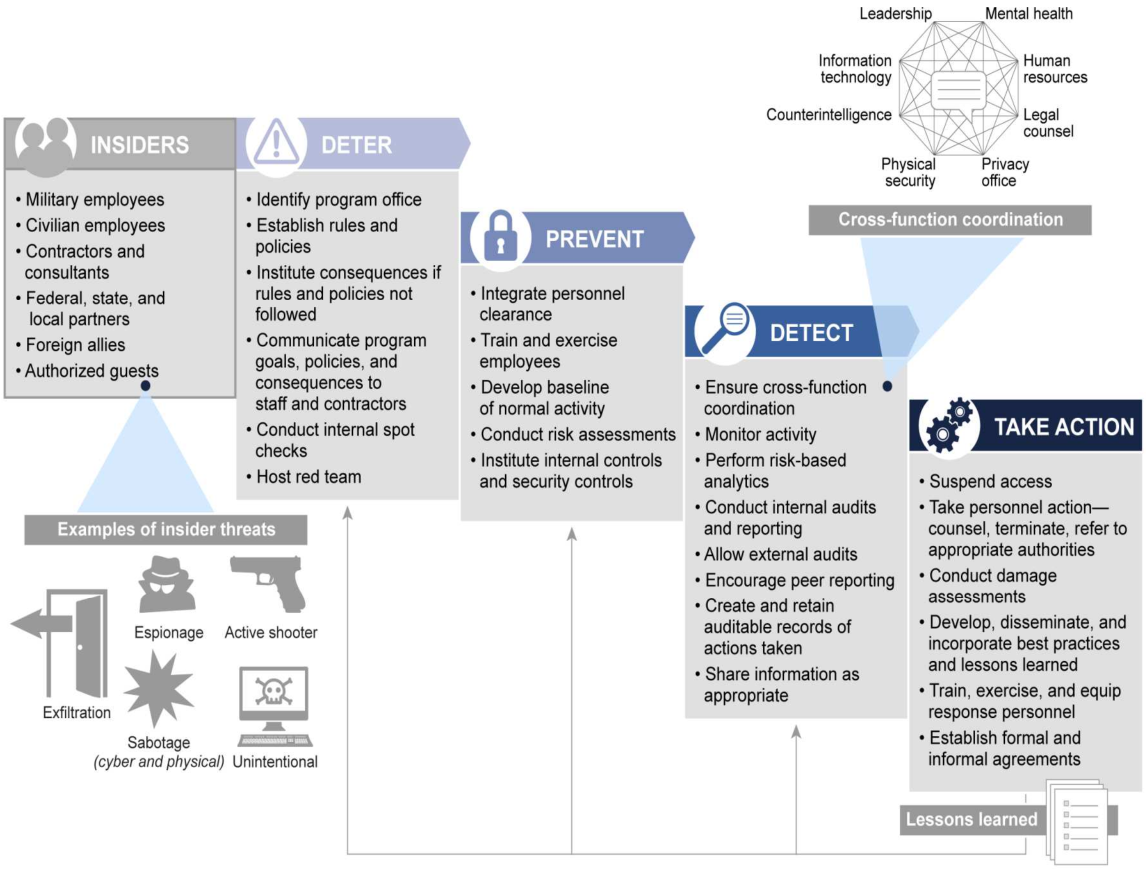
President Obama's 2016 National Counterintelligence Strategy characterized the counterintelligence threat as "daunting" and one that "seeks to undermine our economic strength, steal our most sensitive information, and weaken out defenses" (Committee on Homeland Security House of Representatives One Hundred Fourteenth Congress, 2016, p. 12). Furthermore, DoD places great emphasis on its counterintelligence operations through intelligence collection and analysis by military intelligence commands (i.e. Defense Intelligence Agency, Defense Security Service, etc.). Acting on collected information based on counterintelligence operations is DoD's best defense in thwarting and mitigating insider threats. Therefore, it is important to establish effective counterintelligence efforts.

Policy and Strategic Initiatives

In an effort to mitigate insider threats, the Senior Civilian Official (SCO) of the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) OASD (C3I) established the Insider Threat Integrated Process Team. The Insider Threat Integrated Process Team recommended ten policy and strategic initiatives to thwart insider threats within the DoD. Incorporating effective security education, training, and awareness programs is one of the policies and strategic initiatives that must be developed to improve how personnel identify and report insider threats in the DoD.

GAO identified 25 key elements that DoD should incorporate in their insider threat programs. These key elements are based on a GAO analysis of the National Insider Threat Policy and Minimum Standards for Executive Agencies, DoD policy and guidance, executive-branch policy and reports, and independent studies to mitigate insider threats (Kirschbaum, 2015). Of the 25 key elements, training employees was identified and is an integral part of the "Prevent" phase of DoD's insider threat programs. Additionally, Figure 6 depicts the remaining phases (Deter, Detect and Take Action) as integral parts of insider threat security education and awareness programs.

So far DoD have inconsistently incorporated the following key elements (a) institute and communicate consequences (b) develop a baseline of normal activity (c) share information as appropriate and (d) develop, disseminate and incorporate best practices and lessons learned.


Leadership
Mental health
Information technology
Human resources
Counterintelligence
Legal counsel
Physical security
Privacy office
Cross-function coordination
INSIDERS
• Military employees
• Civilian employees
• Contractors and consultants
• Federal, state, and local partners
• Foreign allies
• Authorized guests
DETER
• Identify program office
• Establish rules and policies
• Institute consequences if rules and policies not followed
• Communicate program goals, policies, and consequences to staff and contractors
• Conduct internal spot checks
• Host red team
PREVENT
• Integrate personnel clearance
• Train and exercise employees
• Develop baseline of normal activity
• Conduct risk assessments
• Institute internal controls and security controls
DETECT
• Ensure cross-function coordination
• Monitor activity
• Perform risk-based analytics
• Conduct internal audits and reporting
• Allow external audits
• Encourage peer reporting
• Create and retain auditable records of actions taken
• Share information as appropriate
TAKE ACTION
• Suspend access
• Take personnel action—counsel, terminate, refer to appropriate authorities
• Conduct damage assessments
• Develop, disseminate, and incorporate best practices and lessons learned
• Train, exercise, and equip response personnel
• Establish formal and informal agreements
Examples of insider threats
Espionage
Active shooter
Exfiltration
Sabotage (cyber and physical)
Unintentional
Lessons learned

Source: GAO analysis of Department of Defense (DOD), U.S. government, and private-sector guidance and reports. | GAO-15-543

Figure 7. Government Accountability Office's framework of key elements to incorporate at each phase of Department of Defense's insider-threat programs.GAO analysis of Department of Defense, U.S. government, and private-sector guidance and reports, GAO-15-543, 2015.

The DoD must implement these recommendations in order to prevent additional insider threat attacks. The shootings at Fort Hood, TX and the Washington Navy Yard could have been prevented if personnel were educated and trained on insider threat awareness. Moreover, managers and military leaders of both individuals involved should have been trained to recognize the characteristics of an insider threat.

In response to the Fort Hood, Texas and Washington Navy Yard shootings, DoD must develop effective training programs and train commanders and supervisors on how to identify behavioral indicators of violence. Security education, training, and awareness programs should take into account lessons learned from these shootings as well as ensure DoD issue interim guidance and provide commanders and supervisors with information and tools needed to identify and respond to insider threats.

A continuing war on terror increases the chance of another insider threat because of the possible influence of Al Qaeda and ISIS among disgruntle personnel with access to classified documentation and information systems (Shaw & Seller, 2015). Although Hasan was a poor performer and displayed erratic behavior, the investigating officer failed to identify signs of radicalization or him as a counterintelligence risk. According to Zegart (2015), DoD's organizational culture of protecting forces from the outside played a role in failing to prevent Hasan from killing 13 people and wounding dozens of others. Despite a rising number of homegrown Jihadi terrorist attacks DoD continues to struggle to adapt to insider threats. Therefore, insider threats like Aaron Alexis, Army Private Bradley Manning, and Army Major Nidal Hasan were prepared to commit hostile acts of violence against DoD personnel and information system (Shaw & Seller, 2015).

Summary and Conclusions

This quantitative research study focuses on the effectiveness of insider threat security education, training, and awareness programs within the DoD. Although Presidential Executive Order 13587 directs the DoD and government agencies to establish insider threat programs based on six minimum standards, the literature identifies several flaws in the system ranging from a lack of effective security education, training, and awareness programs to creating unified databases to track information needed to thwart future insider threat attacks.

Overall, the literature review discussed security education, training and awareness programs, protecting classified information and systems and the implementation of policies and strategic initiatives as means to thwart and mitigate insider threats within the DoD. The use of strategic policies based on the military's intelligence preparation of the battlefield and successfully incorporating organizational culture and change can help DoD leaders understand the importance of mitigating and thwarting insider threats.

The use of current policies and regulations based on recommendations from several investigations conducted by the DoD, FBI and Congress provided the DoD with the necessary tools and resources needed not only to improve but develop better training programs designed to identify and report insider threats. Despite all of the lessons learned from insider threat attacks, DoD leaders must emphasize the importance of identifying and reporting as well as provide better monitoring and information sharing between each military service and government intelligence and law enforcement agencies. Additionally, DoD should consider providing both IBT and CBT as methods of delivering insider threat security education, training and awareness programs.

Chapter 3 will discuss the methodology and threats to validity of this quantitative research study. The methodology section will explain the use of use of sampling procedures based on a target population size to conduct a quantitative research analysis based on two research questions and hypotheses mentioned in Chapter 1. Moreover, the quantitative non-experimental research study will focus on the statistical relationship between two variables as a means of deciding whether or not the effectiveness of insider threat security awareness training in relation to military and civilian personnel understanding how to identify and report insider threats. The section on threats to validity will describe both the external and internal validity and explain how they will be addressed, as well as, the ethical concerns faced by this quantitative research study.

Chapter 3: Research Method

Introduction

For the DoD to mitigate insider threats, personnel must obtain knowledge on insider threat behaviors and characteristics through DoD developed security education, training, and awareness programs. According to the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, which is authorized by Presidential Executive Order 13587, either in-person or CBT to all cleared employees must be conducted within 30 days of initial employment and annually thereafter (DoD Directive 5240.02; DoD, 2015b). Despite the initial and annual training requirement, the DoD identified 87% of insider threats as employees or others internal to the organization (i.e., defense contractors working onsite) who contemplate to divulge classified information (Greitzer & Hohimer, 2011). Additionally, the DoD has not identified a method or system to measure the effectiveness of security education, training, and awareness programs designed to ensure everyone understands the importance of identifying and reporting insider threats within their organizations. Therefore, the purpose of this study was to understand the perceived effectiveness of security education, training and awareness programs provided to DoD personnel.

Chapter 3 is divided into three sections: research design and rationale, methodology, and threats to validity. The Research Design and Rationale section will state the independent, dependent, and controlling and intervening variables; identify research design and its connection to the research questions; explain time and resource constraints; and describe how design choice is consistent with the research design. The

Methodology section will provide an in-depth description of the research so other researchers can replicate the study. This section is subdivided into the following: population; sampling and sampling procedures; procedures for recruitment, participation, and data collection; and instrumentation and operationalization of constructs. And finally, the Threats to Validity section will describe threats to external validity and how they were addressed; describe threats to internal validity and how they were addressed; describe any threats to construct or statistical conclusion validity; and describe the ethical procedures.

Research Design and Rationale

Research design is the defining element of a survey in which the survey results are used to describe the variables being studied (Gravetter & Forzano, 2018). For this study, the research design was quantitative and nonexperimental focused on a limited number of independent and dependent variables. The independent variables were DoD programs (CBT and IBT) designed to mitigate insider threats by changing attitudes, improving knowledge, or increasing skills in identifying an insider threat. The dependent variables were known acts of espionage, unauthorized disclosure of information, and any activity resulting in the intentional or unintentional loss of organizational resources and/or capabilities from the actions of an insider. Control and intervening variables were gender (i.e., male or female) and military and civilian status (e.g., officer, noncommissioned officer, enlisted, DoD civilian, and contractor). The quantitative nonexperimental research design allowed for testing all hypotheses and correlates with the following research questions:

RQ1: What is the perceived effectiveness of CBT and IBT programs in mitigating and thwarting insider threats within the DoD?

RQ2: What is the perceived effectiveness of CBT and IBT programs in preventing known acts of espionage, unauthorized disclosure, or loss of organizational resources?

A nonexperimental research study is focused on a statistical relationship between two variables and does not include the manipulation of the independent variable, nor does it randomly assign participants to conditions or orders of conditions or both (Price, Jhangiani, & Chiang, 2015). The variables in this study were not be manipulated because they are attribute variables such as gender, military rank, DoD civilian status, or contractor. These attributes are reflected in the effectiveness of insider threat security awareness training in relation to military and civilian personnel understanding how to identify and report an insider threat. Additionally, understanding the effects of the DoD organizational culture and change can help leadership mitigate insider threats from their organization.

Methodology

Population

Sampling was necessary in this study because it is not possible to collect data for every individual in the population involving the DoD. The greater the sample size, the more representative is expected to be of the population from which it is drawn (Ary, et. al., 2018). The DoD is the world's largest employer with over 3 million employees located around the world. The target population and sample size consisted of DoD personnel (active, Reserve, and National Guard soldiers, civilians, and contractors) who live and work in the United States and have been employed by the federal government for at least 5 years.

Sampling and Sampling Procedures

The intent of sampling in a quantitative design is to estimate or predict the outcome of a larger population based on data from a sample of that population (Schofield, 2004). In quantitative research studies, sample accuracy represents the larger population and is more important than sample size, as factors that may bias the outcome of the study need to be controlled or excluded (Endacott & Botti, 2005). Hence, identifying the specific characteristics of the target population is the first step in sampling. The next step in the sampling process is to define the inclusion and exclusion criteria of the accessible population. Inclusion criteria are based on the research questions and the research plan and are applied to improve the feasibility of conducting the study. The inclusion criteria for this study are individuals who (a) are current employees of the DoD, (b) have been employed by the DoD for 5 or more years, and (c) completed all of the mandatory annual security training (i.e., Operations Security, Insider Threat, and TARP training). In contrast, exclusion criteria are applied to exclude unique characteristics that may misperceive the results or deal with ethical considerations related to the study. Exclusion criteria for this study included individuals who have been employed by the DoD for fewer than 5 years (i.e., interns, military members in the ranks of E1-E4 and O1-O3).

A quota sample was used to address the research questions and hypotheses based on the independent and dependent variables. The quota sample involved existing participants to recruit future participants from the overall population of the DoD. Nonprobability sample designs such as snowball sampling technique, convenience, purposive, and stratified sampling strategy were not designed to answer the research questions for this study. Additionally, the remaining probability sample designs (simple random, systematic, and cluster sampling) were not suitable for selecting a sample for this study because the target population would not have an equal chance of being selected to participate.

G*Power statistical power analysis was used to determine sample size. G*Power statistical power analysis is a stand-alone power analysis program used in the social behavioral and biomedical sciences to provide both numerical and graphical output options (Faul et al., 2018). Calculating sample size in quantitative research depends on a number of factors including research design, sampling method, the degree of precision required, the variability of the factors being investigated, and the incidence of a particular variable in the population. In general, the larger the sample the higher the likelihood that the findings will reflect the population, resulting in lower sampling error (Endacott & Botti, 2005).

Although there are five types of power analysis in G*Power 3.1.9.2, this study involved a priori analysis to compute the sample size as a function of specified values for the required significance level α, the desired statistical power 1 – β, and the detected population effect size f^2. The sample size was calculated using the G*Power 3.1.9.2 analysis program and the following input: effect size $f^2 = 0.0625$; α err prob = 0.05; and

Power (1-β err prob) = 0.80, resulting in a sample size of 113. Therefore, 113 participants from the DoD were needed to conduct the study.

The following percentages were obtained from the 2015 DoD Demographics Report and used to calculate the simple random samples: 24.5% DoD Civilians, 36.8% Active Duty forces, and 31.2% Ready Reserve (Reserve and National Guard forces). The remaining percentage of 7.5% Defense contractors brings the total demographics percentages to 100%. Therefore, the simple random sample sizes based on a stratified sample size of 113 participants were 28 DoD civilians, 42 Active Duty forces, 35 Ready Reserve forces, and eight Defense contractors.

Procedures for Recruitment, Participation, and Data Collection

Recruiting participants for data collection could have been a challenge because the DoD workforce consists of over 3 million personnel. Therefore, participant recruitment included a subset of the overall DoD workforce population. Additionally, participants (military, civilian, and government contractors) must have completed mandatory security awareness training (i.e., Operations Security training, Insider Threat training, TARP training, etc.) within fiscal year 2018 and been employed by the DoD or defense contractor (contractors only) for 5 or more years. DoD's fiscal year is October 1–September 30.

After gathering a list of potential participants, individuals were contacted via a private message and/or private group invitation. A final review of the list of participants who accept the invitation as compiled. The participants will receive further details regarding the study via private message on the group website setup for this study. During the recruitment phase of the study, each participant was asked for additional contact information (i.e., e-mail, mailing address, etc.) with a limitation on collecting personal identifiable information such as social security number, place of birth, mother's maiden name, date of birth, etc. Although the survey asked a participant's age, date of birth was not be required. Once the contact information was compiled, reviewed, and documented, a detailed letter explaining the study was e-mailed or mailed to each participant.

Additionally, a letter of cooperation was submitted to a DoD organization requesting permission to recruit research participants. The letter explained the study and requested assistance with providing participants for the research study. Once approval from this organization and the institutional review board (IRB) was obtained, a survey link was provided to the organization for dissemination to potential participants.

I planned to collect data for 30 days before closing the study to conduct quantitative analysis on the responses. During data collection, I observed and noted baseline descriptive and demographic characteristics of the sample population as well as how the population is represented in the sample size. The debriefing process consisted of contacting each participant and the DoD organization thanking them for providing their responses to the survey and ensuring them that their identities and responses will be protected as well as the results. The debrief concluded research participation.

Instrumentation and Operationalization of Constructs

The study included a 10-question survey that is aligned to the research questions. Table 2 lists the research questions and corresponding survey questions. A 10-question Likert-scale survey was created using the free online survey tool Survey Monkey. The

Likert-scale survey provided the most reliable way to measure research participants' opinions, perceptions, and behaviors. Likewise, I used Survey Monkey's suite of paid back-end programs, which include data analysis, sample selection, bias elimination, and data representation tools to upload data into SPSS Statistics Software. The advantages to using the Likert-scale survey is that makes question answering easy on the respondent, represents neutral and undecided feelings of participants, the responses are easy to code when accumulating data, and the surveys are quick, inexpensive, and efficient for data collection. The disadvantages to using the Likert-scale survey are that is only gives five to seven options to choose from, and it does not measure the true attitudes of the respondents.

Table 2

Research Survey Questions and Response Options

Survey Questions	Response Options
1. What is your gender?	MALE FEMALE
2. What is your status?	MILITARY O1E – O3E O1 – O3 O4 – O6 O7 – O10 WO1 – CW2 CW3 – CW5 E4 – E6 E7 – E9 CIVILIAN GS7 – GS10 GS11 – GS13 GS14 – GS15 Senior executive service CONTRACTOR
3. How long have you been employed by the DoD or Defense Contractor?	5 -10 Years 10 -15 Year 15 – 20 Years 20 – 25 Years 25 – 30 Years 30+ Years
4. How effective are Computer-based training programs in understanding, identifying and reporting insider threats?	Very Effective Effective Neutral/No Opinion Ineffective Very Ineffective
5. How effective are Instructor-based training programs in understanding, identifying and reporting insider threats?	
6. How effective are Computer-based training programs in identifying and reporting known acts of espionage and unauthorized disclosure?	
7. How effective are Instructor-based training programs in identifying and reporting known acts of espionage and unauthorized disclosure?	
8. How effective are Computer-based training programs in comprehending the importance of mitigating and thwarting insider threats within the DoD?	
9. How effective are Instructor-based training programs in comprehending the importance of mitigating and thwarting insider threats within the DoD?	
10. Overall, DoD annual mandatory insider threat security training, education, and awareness programs are effective.	Strongly Agree Somewhat Agree Neutral/No Opinion Somewhat Disagree Strongly Disagree

Variables, Measurement, and Analytical Method

The independent variables will be DoD CBT versus IBT security education, training, awareness programs designed to mitigate and thwart insider threats in which criterion determines whether or not the effectiveness of security education, training, and awareness CBT or IBT programs changes attitudes, improve knowledge or increase skills in identifying an insider threat. The level of measurement will be the Likert-scale and it will measure the perceived effectiveness of CBT and IBT programs of insider threat security education, training and awareness programs. The dependent variable will be perceived effectiveness. Control and intervening variables will be gender and military and civilian status (e.g., noncommissioned officer, DoD civilian, etc.).

The following research questions and hypotheses will address the relationships between the independent variables and the dependent variables:

RQ1: What is the perceived effectiveness of CBT and IBT programs in mitigating and thwarting insider threats within the DoD?

$H_0$1: There is no statistically significant difference between the perceived effectiveness of CBT and IBT programs in mitigating and thwarting insider threats.

$H_1$1: There is a statistically significant difference between the perceived effectiveness of CBT and IBT programs in mitigating and thwarting insider threats.

RQ2: What is the perceived effectiveness of CBT and IBT programs in preventing known acts of espionage, unauthorized disclosure, or loss of organizational resources?

$H_0$2: There is no statistically significant difference between the effectiveness of CBT and IBT programs in preventing known acts of espionage, unauthorized disclosure, or loss of organizational resources.

$H_1$2: There is a statistically significant difference between the effectiveness of CBT and IBT programs in preventing known acts of espionage, unauthorized disclosure, or loss of organizational resources.

The statistical method used in this research study will be Two-Way Multivariate Analysis of Variance (MANOVA). The Two-Way MANOVA will analyze whether or not the perceived effectiveness of CBT and IBT programs changes attitudes, improve knowledge and increases skills in identifying insider threats among male and female military and civilian personnel.

Threats to Validity

External Validity Threats

Drawing incorrect inferences from sample data can introduce external validity threats. There is a possibility of an interaction of selection and treatment due to the characteristics of the research study participants. Therefore, I must restrict generalization of the groups of participants identified for this research study by distinguishing the characteristics of each group of participants based on the characteristics identified in the research study.

Internal Validity Threats

Internal validity threats in the form of experimental procedures, treatments, or experiences of the participants can interfere with the ability to draw correct inferences form the data about the population in an experiment. Selection and mortality are two forms of internal validity threats that may affect the outcome of this research study.

Selection poses a risk because each of the selected research participants have certain characteristics that may predispose them to a certain outcome. Participants characterized as senior leaders (officers, warrant officers, SES, etc.) are more educated and may have a better understanding of the effectiveness of security education, training, and awareness programs. Whereas subordinates (NCOs/POs, civilians in nonsupervisory positions, etc.) may not take the training as serious or feel it is a way for senior leaders to "check the box" for their annual performance evaluations. Selecting research study participants using the snowball sampling technique works best because research study participants can recruit future participants. Therefore, it is important to ensure all of the research study participants equally understand the importance of security education, training, and awareness programs when it comes to reporting insider threats.

Although the sample size may consist of 113 participants, mortality may become an issue with this research study because participants may decide to drop out of the research study. Ensuring there are enough participants to conduct the research study can reduce the risk of mortality. Therefore, it is crucial that this research study retain a large sample size to minimize the threat of mortality.

Threats to Statistical Conclusion Validity

Additional threats to validity in this research study are possible due statistical validity. There is a possibility to draw inaccurate inferences from the data based on the violation of statistical assumptions or inaccurate statistical power calculations. In order minimize the effects of the statistical threats to validity, I must ensure the data and statistical power are accurate and that there are no violations in my statistical assumptions.

Ethical Procedures

It is important that the research study follow appropriate ethical procedures to protect the participant's privacy. The use of social media as well as a DoD organization with military, civilians and contractors will be used as a source for obtaining potential research study participants. I will discuss my research study with my supervisor and ask for assistance with obtaining permission to recruit participants because this DoD location has the subset or the target population needed to participant in the 10-question research study survey. Additional research participants will be contacted via private messages sent using Facebook and Linkedin. After contacting each individual as well as receiving permission from the DoD organization, I will compile a list of potential research study participants. Each research participant contacted via Linkedin and Facebook will receive a letter via email or mail explaining the research study and asking for their permission to participant in the study. Research participants from the DoD organization will acknowledge their participation in the research study prior to taking the online survey. All research study participants will be given an opportunity to opt out or withdraw from the study at any time. Since the research study will draw from a large population, there should not be any adverse effects to the research study or its findings. Additionally, each participant will be asked to not disclose or discuss the research study. This will be disclosed in the letter provided to the research study participants.

Data will be compiled anonymously and remain confidential throughout the collection phase. I will store data in an encrypted file on a separate external drive and stored in a locked drawer in my home office. I will be the only one with access to the research data. One the research is completed and the dissertation is approved and published I will destroy all hard and digital copies of data collected during the research study.

Summary

The research study will use a large sample size from the DoD to ensure a greater representation of the target population. This includes ensuring the sample size represents the larger population by identifying the specific characteristics of the target population (i.e. military, civilians, and defense contractors). Inclusion and exclusion criteria are based on the research questions, the research plan, are applied to improve the feasibility of conducting the research study and are applied to exclude unique characteristics that may misperceive the results or deal with ethical considerations related to the research study.

The G*Power 3.1.9.2 A priori analysis to compute the sample size as 113 which corresponds to the approximate sample size of 100-120 participants for the research study. Utilizing social media (e.g. Facebook and Linkedin) as well as a DoD organization are great recruitment sources for research participants. Internal and external threats to validity will be addressed by restricting generalizations of groups and by reducing the risk associated with selection and mortality. Whereas threats to statistical conclusion validity will be minimized by the use of accuracy and zero violations in statistical assumptions.

Finally, the research study will follow ethical procedures to ensure each research participant's identity and response remain anonymous and confidential. Digital Research data will be stored in an encrypted data file on an external hard drive and all hard copies will be locked inside a desk drawer in my home office. I will be the only one with access to both digital and hard copy files.

Chapter 4 begins the data collection phase of the research study. After receiving signed letter of permission from each participant and approval from the IRB, I will begin collecting data from research participants using a 10-question survey.

Chapter 4: Results

Introduction

The purpose of this quantitative study was to understand the effectiveness of the security education, training, and awareness programs currently provided to military, civilian, and government contractors with access to DoD resources, organizations, and facilities. I compared the effectiveness of CBT and IBT by exploring the relationships between the independent variables (DoD CBT and IBT programs designed to mitigate insider threats) and the dependent variables (known acts of espionage, unauthorized disclosure of information, and any activity resulting in the intentional or unintentional loss of organizational resources and/or capabilities from the actions of an insider). Control and intervening variables were gender and military and civilian status (e.g., noncommissioned officer, DoD civilian, etc.). Testing these variables helped answer the following research questions:

RQ1: What is the perceived effectiveness of CBT and IBT programs in mitigating and thwarting insider threats within the DoD?

$H_0$1: There is no statistically significant difference between the perceived effectiveness of CBT and IBT programs in mitigating and thwarting insider threats.

$H_1$1: There is a statistically significant difference between the perceived effectiveness of CBT and IBT programs in mitigating and thwarting insider threats.

RQ2: What is the perceived effectiveness of CBT and IBT programs in preventing known acts of espionage, unauthorized disclosure, or loss of organizational resources?

$H_0 2$: There is no statistically significant difference between the effectiveness of CBT and IBT programs in preventing known acts of espionage, unauthorized disclosure, or loss of organizational resources.

$H_1 2$: There is a statistically significant difference between the effectiveness of CBT and IBT programs in preventing known acts of espionage, unauthorized disclosure, or loss of organizational resources.

The DoD workforce consists of over 3 million personnel, making recruitment and data collection a challenge. Although I did not have any issues obtaining approval from a DoD organization to recruit personnel, it was difficult contacting the DoD IRB approval authority as well as obtaining approval to collect data from DoD personnel for my study. After finding the DoD IRB approval authority, I had to obtain IRB approval from Walden University prior to requesting DoD IRB approval to collect data. As a stipulation to receiving DoD IRB approval, I agreed to limit my data collection to 100 participants, though the stratified sample size for my research survey was 113.

Data Collection

Participants were recruited from a sample size of the DoD population of 3 million personnel via a private Facebook Group and a DoD organization. Although the sample size in Chapter 3 was based on a stratified sample size of 113 participants, I was able to recruit 42 research study participants. Forty-two research study participants answered the 10-question Likert-scale survey over a 3-week period from December 10–24, 2019 at a response rate of 1.47 seconds per question. Participants were not required to provide additional contact information (i.e., e-mail, mailing address, etc.), nor were they asked to provide demographics such as age. However, 100% of the participants provided gender, employment status (military, civilian, or defense contractor), and length of employment with the DoD or defense contractor. Five years or more of employment with the DoD or a defense contractor was a criterion for participating in the study.

During the data analysis, I observed and noted baseline descriptive and demographic characteristics of the sample population. The first three survey questions related to demographics and resulted data related to participants' gender, pay grade, and years of employment. Most participants were female (55%), and most were employed for either 5-10 years (29%) or 10-15 years (26%). Finally, most were GS11-GS13 pay grade (76%). Table 3 presents a sample size of the DoD population for personnel who have been employed for 5 or more years. Additionally, the participants are more educated and have a better understanding of the effectiveness of security education, training, and awareness programs.

Table 3

Characteristics of the Survey Respondents (N = 42)

Variable	Frequency (%)
Gender	
Male	19 (45)
Female	23 (55)
Years employed by Department of Defense of as defense contractor	
5-10	12 (29)
10-15	11 (26)
15-20	8 (19)
20-25	2 (5)
25-30	1 (2)
30+	8 (19)
Status by pay grade	
O4-O6	2 (5)
E7-E9	2 (5)
GS7-GS10	2 (5)
GS11-GS13	32 (76)
GS14-GS-15	3 (7)
Contractor	2 (5)

Results

A two-way MANOVA was used to analyze whether the perceived effectiveness of security education, training, and awareness CBT or IBT programs changes attitudes, improve knowledge, and increases skills in identifying insider threats among military and DoD civilian personnel and defense contractors. The descriptive statistics displayed the mean and standard deviation for the dependent variable (perceived effectiveness), which is split by the independent variables (CBT and IBT programs). Descriptive statistics revealed the following: IBT programs (*M* = 1.81, *SD* = .67) are as effective as CBT programs (*M* = 2.26, *SD* = .86) when understanding, identifying, and reporting insider threats. Additionally, IBT programs (*M* = 1.83, *SD* =.66) are as effective as CBT programs (*M* =2.11, *SD* = .74) when identifying and reporting known acts of espionage and unauthorized disclosure. Further, IBT programs (*M* = 1.79, *SD* = .78) are as effective as CBT programs (*M* = 2.26, *SD* = .77) when comprehending the importance of mitigating and thwarting insider threats within the DoD. Overall annual mandatory insider threat security training, education, and awareness programs (M = 1.81, SD = .97) are effective.

Box‘s M Test of Equality of Covariance Matrices was also used to test for homogeneity of variance-covariance matrices. As a result, Box’s M Test of Equality of Covariance Matrices proves that the homogeneity of the variance *F*(28, 2725) = 1.36, *p* = .10 is non-significant. Additionally, Wilks’s Lambda (Λ) was used to test the statistical significance of the different effects of the control and intervening variables (gender and status). The interaction effect determined whether the effect of gender was consistent across different interactions. Alternatively, but equivalently, the interaction effect determined whether the effect of military, DoD civilians, and defense contractors are similar for males and females. If the interaction effect is statistically significant, $p < .05$. Alternatively, if $p > .05$, the interaction effect is not statistically significant. Therefore, it rejects the null hypotheses because there was no statistically significant interaction effect between gender and status on the combined dependent variables, $F(14, 54) = 1.63$, $p = .10$; Wilks's $\Lambda = .49$.

The Tukey test was used to determine the relationship between gender and status and the perceived effectiveness of security education, training, and awareness CBT and IBT programs. Although, the Post hoc test was not performed for gender and status because there were fewer than three groups and at least one group had fewer than two cases, the analyses in Table 5 below displays the perceived effectiveness of security education, training and awareness CBT and IBT programs based on the gender main effect and the gender-by-status interaction effect. The perceived effectiveness of security education, training, and awareness of CBT programs is significant for understanding, identifying, and reporting insider threats, $F(2, 33) = 4.18$, $p = .02$. Additionally, identifying and reporting known acts of espionage and unauthorized disclosure, $F(2, 33) = 3.50$, $p = .04$, whereas it is non-significant for comprehending the importance of mitigating and thwarting insider threats within the DoD, $F(2, 33) = .85$, $p = .43$. Conversely, the perceived effectiveness of security education, training, and awareness IBT programs is significant for identifying and reporting insider threats, $F(2, 33) = 3.26$, $p = .05$. Also, identifying and reporting known acts of espionage, $F(2, 33) = 3.77$, $p =$

.03, whereas it is non-significant for comprehending the importance of mitigating and thwarting insider threats within the DoD, *F*(2, 33) = 3.09, *p* = .06. Overall, DoD annual mandatory insider threat security education, training, and awareness CBT and IBT training is significant, *F*(2, 33) = 6.72, *p* = .004.

The relationships between security education, training, and awareness CBT and IBT programs and the perceived effectiveness in mitigating and thwarting insider threats within the DoD failed to reject the null hypothesis, *F*(2, 33) = 3.09, *p* = .06. In contrast, the relationships between security education, training, and awareness CBT and IBT programs and the perceived effectiveness of preventing know acts of espionage, unauthorized disclosure, or loss of organizational resources rejected the null hypothesis.

Table 4

Perceived Effectiveness of CBT and IBT Programs (N = 42)

Dependent Variable	*M* (*SD*)	*F*(2, 33)	*p*	η^2
CBT				
Reporting IT	2.26(.89)	4.18	.02	.20
ID Espionage	2.12(.74)	3.50	.04	.18
Mitigating IT	2.26(.77)	.85	.43	.05
IBT				
Reporting IT	1.81(.67)	3.26	.05	.17
ID Espionage	1.83(.66)	3.77	.03	.19
Mitigating IT	1.79(.78)	3.09	.06	.16
Overall				
Effectiveness	1.81(.97)	6.72	<.05	.29

Note. IT = insider threat

Finally, Pearson Correlation was conducted to assess the degree that the quantitative variables are linearly related in the sample. According to Green & Salkind (2014), one requirement is to consider the two assumptions are underlying the significance test for the Pearson correlation and then examine the meaning of the Pearson correlation as an effect size statistic. There are the two assumptions. Assumption one is that the variable is bivariately normally distributed. Assumption two is that the cases represent a random sample from the population and the scores on variables for one case are independent of scores on these variables for other cases. According to the statistical analysis, the variables meet both assumptions. Correlation coefficients were computed among security education, training, and awareness CBT and IBT program effectiveness. Table 6 presents the results of the correlational analysis showing 20 out of 21 correlations are statistically significant and were greater than or equal to .50 for *p* < .001 and greater than or equal to .33 for *p* < .005.

Table 5

Correlations Among the Effectiveness of CBT and IBT Programs

Effectiveness	Overall Effectiveness	CBT Report	IBT Report	CBT Espionage	IBT Espionage	CBT Mitigate
CBT Report	.52**					
IBT Report	.47**	.41**				
CBT Espionage	.58**	.73**	.34*			
IBT Espionage	.48**	.58**	.81**	.49**		
CBT Mitigate	.53**	.51**	.15	.55**	.33*	
IBT Mitigate	.52**	.54**	.66**	.43**	.73**	.50**

Note. ***p* < .001
**p* < .005

Summary

The data analysis results addressed the research questions and hypotheses and the relationships between the independent variables and the dependent variables. The outcome of the data analysis failed to reject the null hypothesis for the research questions, resulting in no statistically significant difference in the perceived effectiveness of CBT and IBT programs on mitigating and thwarting insider threats and preventing known acts of espionage, unauthorized disclosure, or loss of organizational resources.

The results from this research study are significant because it aims to explain why the effects of security education, training, and awareness CBT and IBT programs are important to defending the country against foreign and domestic enemies. Also note, that the research participants all agree that both security education, training and awareness CBT and IBT programs are effective in protecting DoD installations and personnel. Chapter 5 will reiterate the purpose and nature of this research study and summarize key findings, provide an interpretation of the findings, describe the limitations of the study and conclude with recommendations for further research on the perceived effectiveness of security education, training, and awareness CBT and IBT programs.

Chapter 5: Discussion, Conclusions, And Recommendations

Introduction

The purpose of this quantitative study was to understand the perceived effectiveness of the security education, training, and awareness programs currently provided to military, civilian, and government contractors with access to DoD resources, organizations, and facilities. Although DoD has several types of security education, training, and awareness programs, I compared the effectiveness of CBT and IBT. A survey was used to assess the benefits and risks of security training, education, and awareness and its effectiveness on identifying and reporting insider threats within the DoD. The independent variables were DoD programs designed to mitigate insider threats, and the dependent variables were known acts of espionage, unauthorized disclosure of information, and any activity resulting in the intentional or unintentional loss of organizational resources and/or capabilities from the actions of an insider (Defense Security Service, 2014).

Interpretation of Findings

Although there is little research about insider threats within the DoD, I was able to obtain literature from GAO reports, presidential executive orders and memorandums, articles from *National Defense* and *Federal Times* journals, U.S. Government policies, laws, and DoD policies and regulations. Past incidents, such as the shootings at Fort Hood, Texas and the Washington Naval Yard, involved individuals who had (a) access to classified information and systems and (b) an intent to harm national security. A recent shooting incident at Pearl Harbor, Hawaii adds to the list of tragic events involving military personnel who are insider threats. But security education, training, and awareness CBT and IBT programs are effective in preventing more tragic incidents.

It is important for institutions to pay attention to patterns of behavior displayed by military members, DoD civilians, and defense contractors as noted in IAD as well as changing DoD's current culture and organizational behaviors as in the theory of organizational culture and change. Both IAD and the theory of organizational culture and change are the best theoretical foundations when it comes to ensuring effective security education, training, and awareness CBT and IBT programs. DoD needs to retain both security education, training, and awareness CBT and IBT programs to ensure insider threats are mitigated and to prevent known acts of espionage, unauthorized disclosure, or loss of organizational resources.

Limitations of the Study

Although the G*Power 3.1.9.2 analysis program was used to calculate the stratified sample size of 113, DoD IRB limited my research participants to 100. However, only 42 DoD personnel volunteered to participant in my study despite invitations via both Linkedin and a DoD organization email invitation. As a result, the non-probability sample size was too small resulting in the study being inconclusive.

Recommendations

The DoD continues to provide the most up to date TARP, CBT, and IBT programs, which is outlined as one of the recommendations in the 2011 GAO report. However, the current administration has not provided any updated presidential executive orders despite the recent insider threat attack at Pearl Harbor, Hawaii. Since the shooting at Pearl Harbor, Hawaii, the DoD is reviewing its current policies and regulations on how it can improve security education, training, and awareness CBT and IBT programs to mitigate insider threats.

Based on recommendations from this study, the DoD needs to continue updating and maintaining its current CBT and IBT programs to ensure incidents, such as the shootings at Fort Hood, Texas, the Washington Naval Yard, and Pearl Harbor, can be prevented. DoD must also learn from the GAO reports, which provide recommendations for improving current and future programs. As for violations of the Espionage Act, the DoD must continue incorporating annual training requirements with emphasis on current and former military, civilian, and defense contractors who commit acts of espionage against the United States. Further, the GAO needs to continue investigating insider threats and providing thorough reports to DoD. Additionally, I recommend DoD conduct an annual review of presidential executive orders and memorandums, laws, and policies and regulations and utilize these documents to improve current and future security education, training, and awareness CBT and IBT programs.

Implications

Protecting classified information and documents from being compromised by insider threats within the DoD protects U.S. citizens from terrorist attacks in the United States and abroad. This research addresses gaps in the literature on the effectives of security education, training, and awareness programs when identifying and reporting insider threats and can provide the DoD with important resources regarding oversight of a sensitive issue. This study was designed to assist the DoD with development and implementation of security education, training, and awareness CBT and IBT programs, which mitigate insider threats. Implications for positive social change include using my analysis to assist the DoD with maintaining and developing programs to protect the warfighters and nation from terrorist threats and attacks. DoD's security education, training, and awareness CBT and IBT programs play an important role in ensuring U.S. citizens live and work in a safe and secure environment.

Conclusion

Security education, training, and awareness CBT and IBT programs are an important part of reporting suspicious activity to protect U.S. installations. Unfortunately, this study is inconclusive because the study did not use a random sample size. The research study data cannot validate the perceived effectiveness of CBT and IBT programs when identifying, reporting, mitigating, and defeating insider threats or preventing known acts of espionage, unauthorized disclosure, and a loss of organizational resources. However, it is important for DoD personnel to report any suspicious activities on or around U.S. installations because it can be the difference between life or death for DoD personnel and their families.

References

Army Regulation 381-12. (2016). Threat awareness and reporting program. Retrieved from https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/AR%20381-12%20FINAL%20WEB.pdf

Baker, C. (2012). *A change of detection: To find the terrorist within the identification of the U.S. Army's insider threat*. Retrieved from https://www-hsdl-org.ezp.waldenulibrary.org/?abstract&did=723130

Blaikie, N. (1993). *Approaches to social enquiry.* Cambridge, MA: Polity Press.

Bunn, M., & Sagan, S. (2014). *A worst practice guide to insider threats: Lessons from past mistakes.* Retrieved from http://www.amacad.org/multimedia/pdfs/publications/researchpapersmonographs/insiderThreats.pdf

Burgess, J. R. D., & Russell, J. E. A. (2003). The effectiveness of distance learning initiatives in organizations. *Journal of Vocational Behavior, 63*(2), 289-303. doi:10.1016/S0001-8791(03)00045-9

CERT Insider Threat Team. (2013). Unintentional insider threats: A foundational study. Retrieved from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=58744

Cherry, J. D. (2010). Information assurance within the United States Air Force. Retrieved from https://eric.ed.gov/?id=ED514498

Coalition Letter to the Inspector General of the Intelligence Community Regarding Insider Threat Program. (2016). Retrieved from http://hdl.handle.net/11213/6098

Defense Security Service Regulation. (2014). *Defense security service insider threat identification and mitigation program.* Retrieved from https://www.dss.mil/documents/about/DSSR_05-06_30Jan14.pdf

Deming, P. T. (2017). *Insider threat: Preventing direct action attacks within the United States Army.* Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/1038631.pdf

Department of Defense. (1999). *DoD insider threat mitigation: Final Report of the insider threat integrated process team*. Retrieved from http://www.dtic.mil/get-tr-doc/pdf?AD=ADA391380

Department of Defense. (2012). Department of Defense Instruction 5240.26: Countering espionage, international terrorism, and the counterintelligence (CI) insider threat. Retrieved from http://fas.org/irp/doddir/dod/i5240_26.pdf.

Department of Defense. (2015a). 2015 Demographics: Profile of the military community. Retrieved from http://download.militaryonesource.mil/12038/MOS/Reports/2015-Demographics-Report.pdf

Department of Defense. (2015b). Department of Defense Directive 5240.02: Counterintelligence (CI). Retrieved from http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/524002p.pdf

Department of Defense. (2017a). Department of Defense Directive 5240.06: Counterintelligence awareness and reporting (CIAR). Retrieved from https://fas.org/irp/doddir/dod/d5240_06.pdf

Department of Defense. (2017b). Department of Defense Directive 5205.16: The insider threat program. Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/520516p.pdf

Department of Defense Science Board. (2012). *Task force report: Predicting violent behavior.* Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a565355.pdf

Easterby-Smith, M., Thorpe, R., & Jackson, P, (2008). *Management research* (3rd ed.). London, England: SAGE.

Endacott, R., & Botti, M. (2005). Clinical research 3: Sample selection. *Intensive & Critical Care Nursing, 21*(1), 51-55. doi:10.1016/j.iccn.2004.11.001

Enlisted Leaders. (2013). *Noncommissioned officer and petty officer: Backbone of the Armed Forces*. Washington, DC: National Defense University Press.

Ericksson, P., & Kovalainen, A. (2008). *Qualitative methods in business research* (1st ed.). London, England: SAGE.

Executive Order 13587. (2011). Structural reforms to improve the security of classified networks and the responsible sharing and safeguarding of classified information. *Federal Register, 76*(198). Retrieved from https://www.archives.gov/files/isoo/policy-documents/eo-13587.pdf

Faul, F., Erdfelder, E., Buchner, A., & Lang, A. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, *41*(4), 1149-1160. doi:10.3758/BRM.41.4.1149

Flynn, M. (2014). Statement before the senate armed services committee United States Senate. Retrieved from http://www.dia.mil/News/Speeches-and-Testimonies/Article-View/Article/567085/2014-annual-threat-assessment/

Gates, R. M. (2010). *Final recommendations of the Fort Hood follow-on-review.*

Retrieved from http://www.handle.dtic.cmil/100.2?/ADA528115

Gelo, O., Braakmann, D., & Benetka, G. (2008), Quantitative and qualitative research: Beyond the debate. *Integrative Psychological Behavior*, *42*, 266-290. doi:10.1007/s12124-008-9078-3

Glasser, J., & Lindauer, B. (2013). Bridging the gap: A pragmatic approach to generating insider threat data. *IEEE Security and Privacy Workshops*. Retrieved from http://www.ieee-security.org/TC/SPW2013/papers/data/5017a098.pdf

Goduka, N. (2012). From positivism to indigenous science: A reflection on world views, paradigms and philosophical assumptions. *Africa Insight*, *41*(4), 123-138. Retrieved from https://www.ajol.info/index.php/ai/index

Government Accountability Office. (2011). *Defense Department cyber efforts: DoD faces challenges in its cyber activities.* Retrieved from https://www.gao.gov/products/GAO-11-75

Government Publishing Office. (2016). Counterintelligence and insider threats: How prepared is the department of homeland security? Retrieved from https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg24382/pdf/CHRG-114hhrg

Green, S. B., & Salkind, N. J. (2014). *Using SPSS for Windows and Macintosh: Analyzing and understanding data* (7th ed.). Saddle River, NJ: Pearson.

Greitzer, F. L., & Hohimer, R. E. (2011). Modeling human behavior to anticipate insider attacks. *Journal of Strategic Security, 4*(2), 25-48. doi:10.5038/1944-0472.4.2.2

Hatch, M. J., & Cunliffe, A. L. (2006). *Organization theory.* Oxford, England: Oxford University Press.

Herbig, K. L. (2017). The expanding spectrum of espionage by Americans, 1947-2015. *PERSEREC Technical Report 17-10.* Retrieved from http://www.dhra.mil/PERSEREC/Selected-Reports/#TR17-10

Jasper, S. E. (2017). U.S. cyber threat intelligence sharing frameworks. *International Journal of Intelligence and Counterintelligence, 30*, 53-65. Retrieved from http://hdl.handle.net/10945/50768

Johnson, N. B. (2013a). Agencies struggle to combat insider threats. *Federal Times*, *49*(17), 1-19.

Johnson, N. B. (2013b). Insider threat programs get off to slow start. *Federal Times*, *49*(19), 1-18.

Kim, P., & Homan, J.V. (2012). Measuring the effectiveness of information security training: A comparative analysis of computer-based training and instructor-based training. *Issues in Information Systems, 13*(1), 215-224. Retrieved from http://iacis.org/iis/2012/49_iis_2012_215-224.pdf

Kirschbaum, J. W. (2015). *Insider threats: DoD should improve information sharing and oversight to protect U.S. installations.*

Lamothe, D. (2016, April 11). The fall of Edward Lin the Navy officer accused of espionage and patronizing a prostitute. *The Washington Post*. Retrieved from https://www.washingtonpost.com

Larter, D. B. (2017, January 22). The strange case of Lt. Cmdr. Edward Lin. *Navy Times*. Retrieved from https://www.navytimes.com

Lincoln, Y.S. & Guba, E.G. (1985). *Naturalistic inquiry.* Newbury Park, CA: Sage.

Magnuson, S. (2014). Funding not following concerns about insider threats. *National Defense Magazine*. Retrieved from http://www.nationaldefensemagazine.org/archive/2014/July/Pages/FundingNotFollowingConcernsAboutInsiderThreats.aspx

Magnuson, S. & Sicard, S. (2015). Experts: Thwarting insider threats takes a holistic approach. *National Defense Magazine*. Retrieved from http://www.nationaldefensemagazine.org/archive/2015/February/Pages/ExpertsThwartingInsiderThreatsTakesAHolisticApproach.aspx

Martinez, L. & Saenz, A. (2013, August 21). *Bradley Manning sentenced to 35 years for leaking secrets.* Retrieved from http://abcnews.go.com/Politics/bradley-manning-sentenced-35-years-leaking-secrets/story?id=20021288.

Noblitt, G.E. & Hare, R.D. (1988). *Meta-ethnography: Synthesizing qualitative studies.* Newbury Park, CA: Sage.

Omar, M. (2015). Insider threats: Detecting and controlling malicious insiders. *New Threats and Countermeasures in Digital Crime and Cyber Terrorism, 8*, 162-172.

Onyanga-Omara, J. & Vanden Brook, T. (2017, May 17). Chelsea Manning, who leaked 700,000 documents to Wikileaks, released from prison. *USA Today*. Retrieved from https://www.usatoday.com/story/news/nation/2017/05/17/chelsea-manning-prison-release/101783186/

Rosenberg, A. (1988). *Philosophy of social science.* Boulder, CO: Westview.

Sabatier, P. A. & Weible, C. M. (Eds.). (2014). *Theories of the policy process* (3rd ed.). Boulder, CO: Westview Press.

Saunders, M, Lewis, P, & Thornhill, A. (2007). *Research methods for business students* (4th ed.). Harlow: Prentice Hall Financial Times.

Savage, C. (2017, January 17). Chelsea Manning to be released early as Obama commutes sentence. *The New York Times*. Retrieved from ttps://www.nytimes.com/2017/01/17/us/politics/obama-commutes-bulk-of-chelsea-mannings-sentence.html.

Shafritz, J. M., Ott, J. S., & Jang, Y. S. (Eds.). (2016). *Classics of organization theory.* (8th ed). Belmont, CA: Wadworth, Cengage Learning.

Stockham, B.E. (2017). *The expanded application of forensic science and law enforcement methodologies in Army counterintelligence*. San Diego, CA: National University.

Stockton, P.N. & Olson, E.T. (2013). *Security from within: Independent review of the Washington Navy Yard shooting.* Washington D.C.: United Stated Department of Defense. Retrieved from https://www.hsdl.org/?view&did=751015.

Subrahmanian, V.S. (2015). *Final report for the DARPA ADAMS project*. College Park, MD: University of Maryland. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a625184.pdf

Tate, J. (2013, August 21). Bradley Manning sentenced to 35 years in WikiLeaks case. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/judge-to-sentence-bradley-manning-today/2013/08/20/85bee184-09d0-11e3-b87c-476db8ac34cd_story.html?utm_term=.ed209ec61e4a

Thiessen, M. (2013, April 16). Soldier sentenced to 16 years in spy case. *Associated Press*. Retrieved from https://www.military.com/daily-news/2013/04/16/soldier-sentenced-16-years-in-spy-case.html

Thompson, L. B. (2015). Insider threat. *Army Magazine, 65*(9), 42-44.

WFMY Staff. (2017, June 3). Navy officer who shared military secrets gets 6 years, kicked out of service. *WFMY News 2*. Retrieved from https://www.wfmynews2.com/article/news/crime/navy-officer-who-shared-military-secrets-gets-6-years-kicked-out-of-service/445414803

What is "Insider Threat?". (2014). *CHIPS Magazine*, 2.

Willemssen, J.C. (2015). *Federal agencies need to better protect sensitive data.* Testimony Before the Subcommittee on Regulatory Affairs and Federal Management, Committee on Homeland Security and Government Affairs, U.S. Senate and the Subcommittee on Oversight and Management Efficiency, Committee on Homeland Security, U.S. of Representatives.

Whitfield, C.L. (2012). *Intelligence fusion paradigm: Understanding complex operational environments implementing the institutional analysis and development framework.* Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a570117.pdf.

Young, S. (2017). Slipping through the cracks: Background investigations after Snowden. *Surveillance & Society, 15*(1), 123-136. Retrieved from http://library.queensu.ca/ojs/index.php/surveillance-and-society/index

Zeadally, S., Yu, B., Jeong, D.H., & Liang, L. (2012). Detecting insider threats: Solutions and trends. *Information Security Journal: A Global Perspective*, 21, 183-192. doi:10.1080/19393555.211.654318