2015

Employees' Perceptions About the Deterrence Effect of Polygraph Examination Against Security Compromises

Joshua Lee Cook
Walden University

Walden University

College of Social and Behavioral Sciences

This is to certify that the doctoral dissertation by

Joshua Cook

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. Mark Stallo, Committee Chairperson,
Public Policy and Administration Faculty

Dr. Mark Gordon, Committee Member,
Public Policy and Administration Faculty

Dr. Tanya Settles, University Reviewer,
Public Policy and Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2015

Abstract

Employees' Perceptions About the Deterrence Effect of Polygraph Examination Against Security Compromises

by

Joshua L. Cook

M.Ed, Strayer University, 2006

BS, Upper Iowa University, 2001

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

December 2015

Abstract

Controversy continues over the use of polygraph testing to deter and detect potential leakers as critics argue that the technique is based on faulty assumptions. The purpose of this descriptive and exploratory research study was to determine whether there was a perceived deterrence effect related to the use of polygraphs between a group of participants who were subjected to a polygraph examination within the past year compared to those who have not experienced a polygraph examination within the same time period. Paternoster and Simpson's, as well as Vance and Siponen's, rational choice models and Bandura's social learning theory served as the theoretical foundation for this study. Specifically, this study assessed groups' perceptions about adhering to security regulations if a polygraph is required, changes in their behavior and attitude, and beliefs about polygraph deterrent effect. Data were obtained through a 15-minute researcher-created survey with a cluster sample of 326 participants. Data were analyzed with a *t* test to determine whether there was a statistically significant difference between the groups. A factor analysis was also conducted. Results indicated that there was a statistically significant difference ($p < .001$) between the groups, suggesting that participants perceive a deterrent effect associated with the use of polygraphs as well as a change of behavior and attitude if a polygraph can be randomly administered at work. The implications for positive social change stemming from this study include recommendations to the nation's national security agencies to continue enforcing the polygraph examinations required of certain security personnel and exploring the possibility of expanding the use of such strategies in order to fortify the national intelligence infrastructure.

Employees' Perceptions About the Deterrence Effect of Polygraph Examination Against Security Compromises

by

Joshua L. Cook

M.Ed, Strayer University, 2006

BS, Upper Iowa University, 2001

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

December 2015

Dedication

This study is dedicated to my family who supported me through this endeavor.

Acknowledgments

I want to thank my family, who provided me continuing and unwavering support throughout this endeavor. I want to thank those who participated in the study and completed the surveys. I also want to acknowledge Mr. Ethnasios Shoukry, who provided his support for this research study. I also want to thank Walden University for providing quality instructors, faculty, and feedback mechanisms which allowed me to learn from my mistakes. Specifically, I would like to thank my Chair, Dr. Mark Stallo, my Committee Member, Dr. Mark Gordon, and my University Research Reviewer, Dr. Tanya Settles, for guiding me through the dissertation process. I would also like to thank Dr. Carolyn Rose-Smith for her outstanding mentorship and support during the dissertation phase.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

The term, insider threats, refers to current or former employees, service providers, or contractors who are the greatest threat to an organization's security management due to their possible noncompliance with security policies (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009; Holmlund, Mucisko, Kimberland, & Freyre, 2010; Holmlund, Mucisko, Lynch, & Freyre, 2011; Jenkins, 2013; Li, Zhang, & Sarathy, 2010). Insider threats can be divided into two categories: (a) nonmalicious and (b) malicious (Jenkins, 2013; Vroom & von Solms, 2004). Nonmalicious insider threats pertain to current and former employees, contractors, and other business partners who put their company at risk because they did not comply with the suggested security policy due to ignorance or nonmalicious negligence (Jenkins, 2013; Vroom & von Solms, 2004). Examples of nonmalicious insider threats include disclosing sensitive information in e-mails or in conversations or visiting websites that are infected with viruses or malware (Holmlund et al., 2010; Jenkins, 2013). On the other hand, malicious insider threats pertain to employees, contractors, and other business partners who have authorized access to their organization's network, system, and data, and intentionally exceeded or misused their access in a way that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems (IS; Computer Emergency Readiness Team [CERT], 2015). Examples of malicious insider threats include stealing and exposing sensitive information, sabotaging systems, and committing financial fraud (Holmlund et al., 2010; Jenkins, 2013).

The health of U.S. companies is vital to the U.S. economy as the economy is a

matter of national security (Figliuzzi, 2012). Based on the Federal Bureau of Investigation's (FBI) pending case load during fiscal year 2012, Figliuzzi (2012), then assistant director of the FBI's Counterintelligence Division, reported that economic espionage losses to the U.S. economy totaled more than $13 billion (para. 1). Ponemon Institute (2011, p. 2) found that the average time to resolve a cyber attack is 18 days, which can cost an organization approximately $415,748. In contrast, Ponemon Institute reported that malicious insider cyber attacks can take more than 45 days to contain.

Different techniques and strategies have been used to deter and detect insider threats, such as human behavioral analysis techniques (e.g., polygraph examinations) and detecting anomalies in system resource utilization (e.g., file access monitoring; Jenkins, 2013; Office of the Director of National Intelligence [ODNI], 2012). However, controversies still continue about the use of polygraph analysis to detect deception (Sylvers & Lilienfeld, 2015). Some supporters argue that it is highly accurate, while some opponents argue that it is very unreliable (American Polygraph Association, 2005; Cumming, 2009; Sylvers & Lilienfeld, 2015). The National Research Council (2003) reported that little is known about whether polygraph screenings are effective in terms of deterring national security crimes. Therefore, in this descriptive and exploratory research study, I determined whether there was a perceived deterrent effect related to the use of polygraphs between a group of participants who were subjected to a polygraph examination within the past year compared to those who have not experienced a polygraph examination within the same time period.

The implications for positive social change are directed at the nation's national security agencies to continue enforcing the polygraph examinations required of certain security personnel and exploring the possibility of expanding the use of such strategies in order to fortify the national intelligence infrastructure. In Chapter 1, I include the background of the study, statement of the problem, purpose of the study, and research questions and hypotheses. In addition, I include the theoretical framework, nature of the study, operational definition of terms, assumptions, scope and delimitations, limitations, significance of the study, and a summary.

Background of the Study

A polygraph is a device that concurrently records a series of different physiological channels (American Polygraph Association, 2013; National Center for Credibility Assessment [NCCA], 2013b). It originated in the late 19th century from research into medical instruments that recorded changes in physiology under a variety of circumstances (Landis & Gullette, 1925; National Research Council, 2003; Trovillo, 1939). When used as a screening device, questions are asked at regular timed intervals and the physiological changes are recorded. Polygraph examiners seek trends based on guidelines in physiological responses to certain types of questions, which often indicate psychological concerns regarding a certain type of question (American Polygraph Association, 2013; NCCA, 2011). The polygraph is used in a variety of settings to detect psychophysiological elements of deception.

A screening polygraph examination is conducted as part of an employment application process or prior to gaining access to certain special programs, such as

operational intelligence platforms and secret military operations programs (U.S. Army, 1993, 1995; U.S. Government, 2013). Federal agencies that use the polygraph to deter and detect unauthorized disclosures include the Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), Department of Energy (DOE), FBI, National Geospatial-Intelligence Agency (NGA), National Reconnaissance Office (NRO), and National Security Agency (NSA; ODNI, 2012). The questions asked on a typical screening polygraph examination are generally standardized throughout the community that uses it (NCCA, 2011; Nelson, 2015). Presumably, the examination is conducted without suspicion of wrong-doing on the part of the examinee. The U.S. Government conducts approximately 40,000 polygraph examinations every year and the majority of the examinations are screening examinations for employment or program access (Koerner, 2002, para. 5; National Research Council, 2003). However, the National Research Council (2003) noted that little is known about whether polygraph screenings are effective in terms of deterring national security crimes.

Deterrence through polygraph screening examinations typically comes in the form of employment avoidance, behavior and attitude change, or behavior maintenance (National Research Council, 2003). According to the National Research Council (2003), individuals will avoid employment at locations where polygraph exams are employed or they will deliberately change prohibited behavior or attitudes in order to comply with the regulations (National Research Council, 2003). While there is an abundance of literature on the reliability and validity of polygraph analysis, there is a lack of research that examines employees' perceptions about the deterrence effect of polygraph analysis.

Therefore, this research study was necessary because it filled that gap and added to the literature regarding this topic.

Statement of the Problem

The reliability of polygraph analysis for detecting deception continues to be a controversial topic (Sylvers & Lilienfeld, 2015). Some supporters have argued that polygraph analysis can detect deception with approximately 80% to 98% accuracy, while many scientists reported that the technique detects deception at rates that are only slightly better than chance (American Polygraph Association, 2005, p. 9; Cumming, 2009, p. 8; Sylvers & Lilienfeld, 2015, p. 1). Until the passage of the Employee Polygraph Protection Act (EPPA) of 1988, many American businesses used polygraph as a tool for screening employees and job applicants (American Polygraph Association, 2005; Cumming, 2009; Sylvers & Lilienfeld, 2015). However, government agencies, contractors working with government agencies, and private-sector employees who are suspected of theft are not exempt from polygraph testing (American Polygraph Association, 2005; Sylvers & Lilienfeld, 2015).

Therefore, one way that U.S. federal agencies (e.g., CIA, DIA, DOE, FBI, NGA, NRO, and NSA) screen for insider threats is through the use of polygraph examinations (Jenkins, 2013; ODNI, 2012). According to the ODNI (2012), Director Clapper announced two steps to better protect sensitive information and further deter and detect potential leakers within the Intelligence Community. This included adding a mandated question related to unauthorized disclosure of classified information to the counterintelligence polygraph and requesting independent investigations of selected

unauthorized disclosure cases. However, critics of polygraph analysis asserted that the technique is based on faulty assumption of a "Pinocchio response," which is a specific physiological lie response or "signature" of deception, as no evidence of such a response has been found (Sylvers & Lilienfeld, 2015, p. 3). Due to the continuing controversy over the use of polygraph testing to deter and detect potential leakers, a descriptive and exploratory research study that determines whether there was a perceived deterrence effect related to the use of polygraphs was needed. The findings of this study can be used to assess whether other detection techniques and mitigation strategies should be used instead.

Purpose of the Study

The purpose of this descriptive and exploratory research study was to determine whether there was a perceived deterrence effect related to the use of polygraphs between a group of participants who were subjected to a polygraph examination within the past year compared to those who either had never experienced a polygraph or the experience was more than a year prior to the distribution of the survey. Deterrence is defined as keeping employees, who have committed or may engage in wrongdoing, out of sensitive positions and keeping employees who are already in sensitive positions from doing undesired activities (National Research Council, 2003). The National Research Council (2003) noted that deterrence is different from the validity of polygraph testing because the polygraph can be an effective deterrent even if it does not provide valid information about deception. Employees' perceptions of the deterrent effects of polygraph testing were measured through the use of a 15-minute researcher-created survey.

Research Questions and Hypotheses

In order to determine whether there was a perceived deterrence effect related to the use of polygraphs, this descriptive and exploratory research study addressed the following research questions:

1. To what extent are there differences in the likelihood to adhere more closely to security regulations if a polygraph is required as a condition of employment by group (no polygraph-treatment vs. polygraph-treatment)?

   $H_0$1: There will be no difference in the likelihood to adhere more closely to security regulations if a polygraph is required as a condition of employment by group (no polygraph-treatment vs. polygraph-treatment).

   H_a1: There will be differences in the likelihood to adhere more closely to security regulations if a polygraph is required as a condition of employment by group (no polygraph-treatment vs. polygraph-treatment).

2. To what extent are there differences in the changing of behavior and attitude if a polygraph can be randomly administered at work by group (no polygraph-treatment vs. polygraph-treatment)?

   $H_0$2: There will be no differences in the changing of behavior and attitude if a polygraph can be randomly administered at work by group (no polygraph-treatment vs. polygraph-treatment).

   H_a2: There will be differences in the changing of behavior and attitude if a polygraph can be randomly administered at work by group (no polygraph-treatment vs. polygraph-treatment).

3. To what extent are there differences in the belief that a polygraph is an effective deterrent against security compromises by group (no polygraph-treatment vs. polygraph-treatment)?

   $H_0$3: There will be no differences in the belief that a polygraph is an effective deterrent against security compromises by group (no polygraph-treatment vs. polygraph-treatment).

   H_a3: There will be differences in the belief that a polygraph is an effective deterrent against security compromises by group (no polygraph-treatment vs. polygraph-treatment).

Theoretical Framework

Paternoster and Simpson's (1996) rational choice model of corporate crime, Vance and Siponen's (2012) rational choice model, and Bandura's (1974, 1977, 1986) social learning theory (SLT) served as the theoretical foundation for this study. A brief overview of the theories is provided in this section with a more detailed explanation provided in Chapter 2. This section is organized in the following subsections: Paternoster and Simpson's rational choice model, Vance and Siponen's rational choice model, and SLT.

Paternoster and Simpson's Rational Choice Model

The Paternoster-Simpson rational choice model of corporate crime is essentially a subjective expected utility theory (Paternoster & Simpson, 1996). Paternoster and Simpson (1996) reported that the model is based on two assumptions: "(1) Decisions to offend are made on a balancing of both the costs and benefits of offending and (2) what

are important are the decisionmaker's perceived or subjected expectations of reward and cost" (p. 553). The researchers related that the first assumption pertains to individuals being at least minimally rational agents and their conduct being partly guided by the expected consequences of their behavior. In regard to the second assumption, they noted that an implication is made that the critical agent of corporate crime is the individual. The researchers suggested that the decision to break the law is made by individuals; however, these individuals are affected by the context in which they are employed and commit their crimes. Hence, employees who commit corporate crimes are affected by the characteristics and imperatives of their business organization. Specifically, the decisions of employees are influenced by (a) the risks and benefits they perceive for themselves, (b) the risks and benefits they perceive for their company, and (c) the presence or absence of offending inducements or restrictions within the specific context of the organization.

Vance and Siponen's Rational Choice Model

In order to better understand the effect of expected benefits on IS security violations, Vance and Siponen (2012) used Paternoster and Simpson's (1996) rational choice model as the basis for their theoretical model. Vance and Siponen reported that rational choice theory (RCT) had not been used in the field of IS. The researchers related that RCT explains individuals' decisions to commit crimes as utilitarian calculations based on perceived benefits and both formal and informal sanctions. Therefore, RCT extends beyond deterrence theory by including individuals' perceptions of benefits of violations and informal sanctions, and espoused moral beliefs. They noted that RCT is commonly used to explain criminal behavior; however, it is general enough to cover all

violations. Vance and Siponen noted that RCT is also applicable to the study of violations of organizational IS security policies. The researchers also noted that RCT has been found to explain white-collar crimes better than street-level crimes. Due to this and because RCT has been found to be effective in the corporate context (e.g., Paternoster & Simpsons, 1996), Vance and Siponen related that they expected it to be a good fit for explaining intentional IS security policy violations, which also includes a deliberate violation of organizational norms.

To better explain IS security policy violations in situations where employees are aware of the IS security policy, Vance and Siponen's (2012) theoretical model includes disincentives (sanctions) and incentives (perceived benefits) for violating IS security policies. In addition, their model includes both informal sanctions, which are unstated social penalties; formal sanctions, which are explicit penalties for specific forms of misconduct; and moral beliefs. The researchers' RCT model includes formal sanctions, informal sanctions, moral beliefs, and perceived benefits.

Social Learning Theory

Bandura (1974, 1977, 1986) developed SLT in the 1960s, which was later changed to social cognitive theory (SCT) in 1986 (Boston University School of Public Health, 2013). According to the Boston University School of Public Health (2013), SLT posits that learning occurs in a social context with a three-way, dynamic, and reciprocal interaction of the person, environment, and behavior. In this theory, focus is placed on social influence and external and internal social reinforcement (Boston University School of Public Health, 2013). In SLT, consideration is placed on the unique way in which

individuals acquire and maintain behavior, while considering the social environment in which individuals perform the behavior (Boston University School of Public Health, 2013). The theory takes into account individuals' past experiences, which influences reinforcement, expectations, and expectancies (Boston University School of Public Health, 2013). All of these factors shape whether individuals will engage in a specific behavior and the reasons for doing so.

SLT's goal is to explain how individuals regulate their behavior through control and reinforcement to achieve goal-directed behavior that can be maintained over time (Boston University School of Public Health, 2013). Boston University School of Public Health (2013, para. 3) discussed six constructs of SLT: (a) reciprocal determinism, (b) behavioral capability, (c) observational learning, (d) reinforcements, (e) expectations, and (f) self-efficacy. These constructs are discussed in further detail in Chapter 2.

Nature of the Study

This descriptive and exploratory research study determined whether there was a perceived deterrent effect related to the use of polygraphs between a group of participants who were subjected to polygraph examination within the past year compared to those who have not experienced a polygraph examination within the same time period. This research design was appropriate as the goal of the research study was to determine whether there was a statistically significant difference between the polygraph-treatment and no polygraph-treatment groups' perceptions of the deterrence effect of polygraph examinations.

The 152 participants in the polygraph-treatment group had taken the polygraph through the U.S. Army Intelligence Polygraph Program, which has offices in South Korea and Fort Meade, Maryland. The 174 participants in the no polygraph-treatment group were nonintelligence U.S. citizens and legal resident aliens who lived and worked in South Korea, were students from the Walden University participant pool, and individuals from the Walden University online community site, LinkedIn. Data were obtained through a 15-minute researcher-developed questionnaire. Data were analyzed using SPSS, which included descriptive statistics, such as means and standard deviations. A *t* test was used to determine whether there was a statistically significant difference between the groups. In addition, a factor analysis was conducted among the 30 polygraph questions. The nature of the study is discussed in further detail in Chapter 3.

Operational Definition of Terms

Counterintelligence: Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorist activities (NCCA, 2011).

Deterrence: "Keeping people who have done or may do certain undesired things out of sensitive positions and keeping people already in sensitive positions from doing undesired things" (National Research Council, 2003, p. 53).

Insider threats: Refers to current or former employees, service providers, or contractors who are the greatest threat to an organization's security management due to their possible noncompliance with security policies (Boss et al., 2009; Holmlund et al.,

2010; Holmlund et al., 2011; Jenkins, 2013; Li et al., 2010).

Intelligence: Information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons (Executive Branch, 2008; U.S. Government, 2013).

Leak: An unauthorized disclosure of controlled or classified government information, often to the open press for publication, which is a deliberate security compromise (Elsea, 2013).

Lie detector: "Includes a polygraph, deceptograph, voice stress analyzer, psychological stress evaluator or similar device (whether mechanical or electrical) used to render diagnostic opinion as to the honesty of an individual" (U.S. Department of Labor [DOL], 2008, para. 3).

Malicious insider threats: Pertains to employees, contractors, and other business partners who have authorized access to their organization's network, system, and data and intentionally exceeded or misused that access in a way that negatively affected the confidentiality, integrity, or availability of the organization's information or IS (CERT, 2015).

National Center for Credibility Assessment (NCCA): U.S. government's premiere educational center for polygraph and other credibility assessment technologies and techniques (NCCA, 2013a). Its central mission is to assist federal agencies in the protection of U.S. citizens, interests, infrastructure, and security by providing the best education and tools for credibility assessment (NCCA, 2013a).

Nonmalicious insider threats: Pertains to current and former employees,

contractors and other business partners who put their company at risk because they did not comply with the suggested security policy due to ignorance or nonmalicious negligence (Jenkins, 2013; Vroom & von Solms, 2004).

Paternoster and Simpson's rational choice model: Is based on two assumptions: "(1) Decisions to offend are made on a balancing of both the costs and benefits of offending and (2) what are important are the decisionmaker's perceived or subjected expectations of reward and cost" (Paternoster & Simpson, 1996, p. 553).

Polygraph: "An instrument that records continuously, visually, permanently, and simultaneously changes in cardiovascular, respiratory and electrodermal patterns as minimum instrumentation standards and is used to render a diagnostic opinion as to the honesty or dishonesty of an individual" (DOL, 2008, para. 3). An examinee is asked a series of questions and the results are often used in making determinations about access to classified information or programs, or assist in determining examinee's involvement in a specific issue (American Society for Testing and Materials (ASTM) International, 2005; U.S. Department of Defense [DOD], 2006; NCCA, 2011).

Polygraph examination: A process that encompasses all activities that take place between a polygraph examiner and an examinee during a specific series of interactions (NCCA, 2011; Nelson, 2015).These interactions may include the pretest interview, the use of the polygraph instrument to collect physiological data from the examinee while presenting a series of tests, the test data analysis phase, and the posttest phase, which may include the interrogation of the examinee (NCCA, 2011; Nelson, 2015).

Polygraph examiner: Someone who has successfully completed formal education

and training in conducting polygraph examinations and is certified by their agency to conduct such examinations. Army Polygraph Examiners must possess at a minimum counterintelligence special agent training, 2 years investigative experience, a bachelor's degree, completion of the Psychophysiological Detection of Deception (PDD) School, and successful completion of at least 6 months as an intern (ASTM International, 2005; NCCA, 2011).

Polygraph test: A portion of the polygraph examination, often called the in-test, in which a series of questions are administered, with a polygraph instrument collecting physiological information from an examinee, and an analysis is conducted in an effort to determine the likelihood of guilt or innocence (NCCA, 2011; Nelson, 2015).

Relevant questions: Questions used during a polygraph that are intended to be the focus of the polygraph. Examples of relevant questions are: Have you committed espionage against the United States and did you stab that person? (NCCA, 2011; Nelson, 2015)

Screening exam: A multiple relevant issue polygraph test that is given to a population without any specific accusation (NCCA, 2011; National Research Council, 2003; Nelson, 2015).

Social learning theory (SLT): SLT posits that learning occurs in a social context with a three-way, dynamic, and reciprocal interaction of the person, environment, and behavior (Boston University School of Public Health, 2013).

U.S. Intelligence Community: Coalition of 17 agencies and organizations within the executive branch that work both independently and collaboratively to gather the

intelligence necessary to conduct foreign relations and national security activities (ODNI, 2015b).

Vance and Siponen's rational choice model: Explains individuals' decisions to commit crimes as utilitarian calculations based on perceived benefits and both formal and informal sanctions (Vance & Siponen, 2012). It also includes individuals' perceptions of benefits of violations and informal sanctions, and espoused moral beliefs (Vance & Siponen, 2012). Thus, their model includes formal sanctions, informal sanctions, moral beliefs, and perceived benefits (Vance & Siponen, 2012).

Assumptions

Assumptions made for this study were:

- The 15-minute researcher-created questionnaire was appropriate for assessing the perceived deterrence effect related to the use of polygraphs among the two groups.
- The survey was worded so that the participants could accurately interpret the information being asked and the participants provided their honest perceptions.
- The individuals who were recruited and received the hard copy consent form and the survey link were the ones who completed the survey.
- The surveys accurately measured what they are intended to measure.
- Employees were willing to take part in the study because of its significance.
- The results of the study will lead to positive social change by further enforcing polygraph examinations and exploring the possibility of expanding the use of such strategies.

Scope and Delimitations

The study only focused on the perceived deterrence effect related to the use of polygraphs. It did not focus on the validity, reliability, or accuracy rates of polygraph examinations. The study applied to employees who are U.S. citizens and resident aliens in the United States and South Korea. Employees in the polygraph-treatment group had taken the polygraph within the past year through the U.S. Army Intelligence Polygraph Program, which has offices in South Korea and Fort Meade, Maryland. Employees in the no polygraph-treatment group were individuals who had not taken a screening polygraph examination in the last year and who were not required to take a polygraph as part of their job requirements. They were nonintelligence personnel who lived in South Korea, students from the Walden University participant pool, and individuals from the Walden University online community site, LinkedIn. Excluded were individuals under the age of 18 and individuals who had pending polygraph examinations with me in order to prevent a possible conflict of interest or perceived quid pro quo bias.

Limitations

This study had several limitations. First, this study determined the perceived deterrent effect related to the use of polygraphs between two groups; therefore, the study remained distinct in its focus and limited in its scope. This study was not designed to answer questions related to the validity, reliability, or accuracy rates of polygraph examinations. Although these topics may be important to public policy and the administration field, the psychology field, and the intelligence community, they were not the focus of this research effort.

A second possible limitation of the study includes generalizing the results since a cluster sampling of 326 participants, all of whom were U.S. citizens or legal resident aliens located in South Korea and the United States, was used and the results of the study are limited to similar populations of employees. The 152 participants in the polygraph-treatment group had taken the polygraph through the U.S. Army Intelligence Polygraph Program, which has offices in South Korea and Fort Meade, Maryland. The 174 participants in the no polygraph-treatment group were nonintelligence U.S. citizens and legal resident aliens who lived and worked in South Korea, were students from the Walden University participant pool, and individuals from the Walden University online community site, LinkedIn. These employees' unique perceptions may not be generalizable to other populations.

Third, I used a 15-minute researcher-developed survey, which has not been used in past studies. However, a pilot study was conducted on the survey prior to using it in the main study. In developing the questions used in the survey, I received assistance from two agencies, the NCCA and the U.S. Army Intelligence Polygraph Program. To help establish the validity of the survey, a member of the research department of the NCCA and a retired polygraph examiner and former employee of the CIA also reviewed the survey questions and provided additional comments to the proposed questions to ensure consistency with community standards. In addition, the survey was found to have very high reliability (Cronbach's alpha = >.90).

Fourth, selection or sampling bias was another limitation of the study. In regard to selection bias, since I am a polygraph examiner and some of the participants received

their screening examination from me, participants may expect preferential treatment. However, participants were informed on the consent form that there were no connections between the study and their examination; therefore, they should not expect any preferential treatment as a result of their voluntary participation in the study. Future research could exclude participants who have taken a polygraph from the researcher. In addition, changes to the populations could be made in future research, where more similar populations are compared. Specifically, two similar groups of participants who work only in the intelligence community, one group who require polygraph testing within the last year against those who either had never experienced a polygraph or the experience was more than a year prior, could be compared and the results compared to the findings found in this study.

A fifth limitation was nonresponse bias. Nonresponse bias could have resulted in a low response rate on the survey and a decrease in the sample size, which could also affect the generalizability of the data. Some surveys could not be used as some participants did not complete all the questions. However, there was enough participation to meet the sample size needed, where 300 participants was the minimum and 326 individuals participated in the study.

A sixth limitation was self-report or social desirability bias. Self-report or social desirability bias has to be considered as participants may want to be perceived positively so they may not respond honestly. In addition, there are problems inherent with self-report data as participants may not accurately or fully self-evaluate themselves. In order to address this bias, the Likert scale format was used, which did not allow participants the

freedom to include additional information that they may have felt was important. In addition, it was assumed that participants answered honestly to the questions asked on the survey.

Significance of the Study

While there is an abundance of literature on the reliability and validity of polygraph analysis, this research study added to the literature and advanced knowledge by filling a gap in the public policy and administration literature with respect to employees' perceptions about the deterrence effect of polygraph analysis. Findings from this study are beneficial not only to the public policy and administration field, but to a wide array of other fields, including the fields of psychology and intelligence. The findings from the study are also applicable to many agencies and organizations, to include the DOD and the coalition of 17 agencies and organizations that are a part of the U.S. Intelligence Community including the ODNI, Army Intelligence, FBI, and CIA.

The findings from this study also advanced practice and policy. Based on these findings, there was a perceived deterrence effect related to the use of polygraphs between the two groups. Employees in sensitive positions who face random polygraph testing may take greater care to avoid even minor security infractions in order to avoid the possibility of a future deceptive reading on a polygraph test. One of the goals of polygraph testing is deterrence, which means keeping employees, who have committed or may engage in wrongdoing, out of sensitive positions and keeping employees who are already in sensitive positions from doing undesired activities (National Research Council, 2003). The findings of Research Question 2 that random polygraph testing may result in a

change of behavior and attitude is significant as it may deter actions that threaten national interests based on the perceived likelihood and consequences of detection. Therefore, the implications for positive social change stemming from these findings include recommendations to the nation's national security agencies to continue enforcing the polygraph examinations required of certain security personnel and exploring the possibility of expanding the use of such strategies in order to fortify the national intelligence infrastructure.

Summary

The focus of this study was on whether there was a perceived deterrent effect related to the use of polygraphs between a group of participants who were subjected to a polygraph examination within the past year compared to those who have not experienced a polygraph examination within the same time period. Data were collected through the use of a 15-minute researcher-created questionnaire with 326 volunteer participants, all of whom were U.S. citizens or legal resident aliens located in South Korea and the United States. Data were analyzed using SPSS and data analysis included the use of descriptive statistics, a *t* test, and a factor analysis. Findings from this study may advance practice and policy by further encouraging policymakers and the nation's national security agencies to continue enforcing the polygraph examinations required of certain security personnel and exploring the possibility of expanding the use of such strategies in order to fortify the national intelligence infrastructure.

In Chapter 1, I included the introduction, background of the study, statement of the problem, purpose of the study, research questions and hypotheses, theoretical

framework, nature of the study, operational definition of terms, assumptions, scope and delimitations, limitations, significance of the study, and a summary. In Chapter 2, I include the introduction, literature search strategy, theoretical foundation, background of polygraph testing, Employee Polygraph Protection Act of 1988, polygraph as a deterrent against security compromises, polygraph's effect on employees' behavior and attitudes, adhering to security regulations due to polygraph, and a summary and conclusions. In Chapter 3, I include the introduction, research design and rationale, methodology, data analysis plan, threats to validity, and a summary. In Chapter 4, I include the introduction, pilot study, data collection and study results, and a summary of the chapter. In Chapter 5, I include the introduction, interpretation of findings, limitations of the study, recommendations, implications, and a conclusion to the study.

Chapter 2: Literature Review

Introduction

In this descriptive and exploratory research study, I determined whether there was a perceived deterrence effect related to the use of polygraphs between a group of participants who were subjected to a polygraph examination within the past year compared to those who either had never experienced a polygraph or the experience was more than a year prior to the distribution of the survey. Controversy over the use of polygraph testing to deter and detect potential leakers continues (National Research Council, 2003; Sylvers & Lilienfeld, 2015). Some polygraph proponents claim that the polygraph technique is highly accurate and can detect deception with approximately 95% accuracy (American Polygraph Association, 2005, p. 5; Sylvers & Lilienfeld, 2015, p. 1). However, some scientists argue that the polygraph technique only detects deception at a rate that is slightly better than chance (Sylvers & Lilienfeld, 2015).

As the FBI's economic caseload increases, so does the percentage of cases that are attributed to insider threats, where current or former trusted employees, contractors, and other business partners are a growing part of the problem (Figliuzzi, 2012). Figliuzzi (2012) highlighted a 2012 indictment, where several former employees who had more than 70 combined years of service working for a company were convicted of selling trade secrets on the production of titanium dioxide to a competitor in China. Figliuizzi emphasized that this case was one of the largest economic espionage cases in the FBI's history. In Chapter 2, I include the literature search strategy, theoretical foundation, background of polygraph testing, Employee Polygraph Protection Act of 1988, polygraph

as a deterrent against security compromises, polygraph's effect on employees' behavior and attitudes, adhering to security regulations due to polygraph, and a summary and conclusions.

Literature Search Strategy

The literature search included an in-depth search in Walden University Library research databases, including all EBSCOhost databases and ProQuest. Databases included ProQuest Criminal Justice, Political Science Complete, Political Science Complete, Oxford Criminology Bibliographies, International Security and Counter Terrorism Reference Center, Military and Government Collection, PsycINFO, and PsycARTICLES. Organizational websites were also searched such as Secrecy News found on the Federation of American Scientists website. Search terms included *deception, polygraph*, *lie detection, detection of deception, polygraph and employees, polygraph and deterrence effect*, *polygraph and behavior and attitude, social learning theory, rational choice theory*, *deterrence theory*, *deterrence*, and *crime prevention through deterrence.*

Theoretical Foundation

Paternoster and Simpson's (1996) rational choice model of corporate crime, Vance and Siponen's (2012) rational choice model, and Bandura's (1974, 1977, 1986) SLT can be used to understand deterrence effects in the workplace. I discussed the theoretical propositions of the theories and how they have been applied previously in ways similar to this study. This section is organized in the following subsections: rational choice theory and social learning theory.

Rational Choice Theory

In this subsection, I discussed Paternoster and Simpson's (1996) rational choice model. In addition, I discussed Vance and Siponen's (2012) rational choice model. It is organized in the following areas: overview, Paternoster and Simpson's rational choice model, Vance and Siponen's rational choice model, and research application of rational choice theory.

Overview. Numerous theorists have been credited with establishing RCT, such as Homans (1961), who created a basic framework of exchange theory by using assumptions drawn from behaviorist psychology (Scott, 2000). However, other theorists, such as Blau (1964), Coleman (1973), and Cook (1977), have expanded on Homans's framework, and developed more formal, mathematical models of RCT (Scott, 2000). In addition, Li et al. (2010) reported that Becker (1968) originally developed RCT with the premise that offenders weigh the costs and benefits in deciding whether to offend. The researchers noted that Becker's premise has been adapted to various contexts to explain deviant behavior and that Paternoster and Simpson (1996) further refined the theory to explain corporate crimes or deviant behaviors in the workplace.

Paternoster and Simpson's rational choice model. RCT has been found to be useful in understanding corporate crime or deviant behaviors in the workplace because both corporate crime and corporate offenders are thought to be particularly amenable to sanction threats (Paternoster & Simpson, 1996). As a result, Paternoster and Simpson (1996) related that they extended the rational choice model to study employees' deviant behaviors in the workplace. The researchers argued that past research has generally

focused on the deterrent effect of formal sanction threats, but the relevance of other potential costs of offending such as loss of occupational position, social censure, personal embarrassment, and shame, have not been explicitly included in a comprehensive test of RCT of corporate crime. The researchers argued that a more comprehensive empirical test of corporate crime that explicitly considers the complete range of available sanctions and rewards of corporate offending, as well as the notion of self-censure and morality was needed. Subsequently, Paternoster and Simpson noted that they developed a rational choice model of corporate crime based in part on Becker's (1968) neoclassical economic theories of crime.

The Paternoster-Simpson rational choice model of corporate crime is essentially a subjective expected utility theory (Paternoster & Simpson, 1996). Paternoster and Simpson (1996) reported that the model is based on two assumptions: "(1) Decisions to offend are made on a balancing of both the costs and benefits of offending and (2) what are important are the decisionmaker's perceived or subjected expectations of reward and cost" (p. 553). The researchers related that the first assumption pertains to individuals being at least minimally rational agents and that their conduct is partly guided by the expected consequences of their behavior. In regard to the second assumption, the researchers noted that an implication made is that the critical agent of corporate crime is the individual. The researchers suggested that the decision to break the law is made by individuals; however, these individuals are affected by the context in which they are employed and commit their crimes. Hence, employees who commit corporate crimes are affected by the characteristics and imperatives of their business organization.

Specifically, the decisions of employees are influenced by (a) the risks and benefits they perceive for themselves, (b) the risks and benefits they perceive for their company, and (c) the presence or absence of offending inducements or restrictions within the specific context of the organization.

The exact form that costs and benefits of corporate crime may take varies (Paternoster & Simpson, 1996). Paternoster and Simpson (1996) argued that the company's cost could include regulatory, civil, and criminal sanctions; reduced revenue; decreased ability to compete against foreign competitors; or a decrease in the company's prestige. The company's benefit could include increased revenues and prestige and the opportunity to challenge the perceived unnecessary regulation or law. On an individual level, the cost of corporate crime also includes the possibility of formal legal sanction such as civil or criminal sanctions; reduced prestige of the organization where the individual works; loss of self-respect; and social censure from colleagues, family, and friends. The benefits on an individual level would include career advancement and an increase in personal income. Therefore, what is beneficial and costly to the company is also beneficial and costly to employees.

Furthermore, in additional to instrumental concerns, employees' decisions to commit corporate crime may be affected by normative factors such as their moral evaluation of the act (Paternoster & Simpson, 1996). According to Paternoster and Simpson (1996), employees may be restrained by moral inhibitions; therefore, some acts of corporate crime are not committed because they are believed to be wrong. The researchers discussed how normative restraints fit into the neoclassical rational choice

model from their perspective. First, the researchers related that norms act as constraints on employee decision makers, restricting the range of available choices. Second, the researchers view this restraint as noninstrumental; therefore, moral inhibitions are not based on the consequences of employees' behavior. Employees do not behave a certain way because of the expected outcomes or because it is expected of others; instead, moral rules are internalized.

Subsequently, certain acts are not committed because it is believed to be morally correct not to commit them (Paternoster & Simpson, 1996). Paternoster and Simpson (1996) drew two implications from this for the role of moral evaluations in conduct. First, the researchers reported that employees' moral beliefs restrain conduct that is deemed to be impressible independent of considerations of cost and benefit. Therefore, Paternoster and Simpson noted that moral considerations play a significant independent role in maintaining conforming conduct. Second, moral considerations should condition the impact of instrumental ones. Specifically, the researchers argued that considerations of cost and benefit do not affect those acts already strongly inhibited by notions of morality. Paternoster and Simpson reasoned that employees' moral sentiments expressly set some behaviors off limits, making them taboo. The taboos are observed due to moral duty and not subject to calculations of utility.

Employees' decisions to commit corporate crime may be affected by the context or circumstances of the organization (Paternoster & Simpson, 1996). Paternoster and Simpson (1996) suggested that employees may be more apt to commit corporate crime if they perceive the company is losing its competitive edge, suspect the overall economic

health of the organization is declining, or the moral climate of the organization tolerates or encourages such misconduct. However, the researchers noted that employees may be dissuaded from offending if the organization or a staff member has recently been sanctioned for similar conduct or the company has organizational restraints such as an ethics hotline.

In testing their proposed rational choice model of corporate crime, Paternoster and Simpson (1996, pp. 555-556) discussed the subjective rewards and costs of corporate criminal conduct as perceived by individual decision makers, which include the following:

1. Formal sanction threats: Directed against the company and employees.
2. Informal sanction threats: Directed against the company and employees.
3. Self-imposed punishment: Shame.
4. The perceived benefits of noncompliance: For the company and employees.

In addition, each employees' personal stock of moral beliefs about specific forms of corporate crime also needs to be assessed (Paternoster & Simpson, 1996). Paternoster and Simpson (1996) also noted that consideration should be given to the context of the organization, its competitive status, its moral climate, and its previous experience with corporate or employee sanctions for misconduct. In summary, the researchers argued that intention to commit corporate crime is a function of the following factors (Paternoster & Simpson, 1996, p. 556):

1. Perceived benefits of the action for oneself.
2. Perceived formal and informal sanctions directed against oneself.

3. Feelings of shame or self-imposed punishment.
4. Moral inhibitions against committing the act.
5. Perceived benefits of the action for the organization.
6. Perceived formal and informal sanctions directed against the organization.
7. Perceived loss of prestige for the organization.
8. The organizational context of the company.
9. Characteristics of the organization.

Data in Paternoster and Simpson's (1996, p. 557) study were collected from 84 business students who were potentially at risk for committing corporate crime and 12 executives who were currently at risk for such crime. However, the total sample size was noted to be 384 because each person read and responded to four different scenarios where they described the commission of corporate crime ($96 \times 4 = 384$; Paternoster & Simpson, 1996, p. 557). The researchers found considerable support for a rational choice model that included an appeal to both rationality and morality. Findings indicated that intentions to commit four types of corporate crime were affected by formal and informal sanction threats, moral evaluations, and organizational factors (CITE). Based on their findings, Paternoster and Simpson suggested a number of alternative but compatible strategies for dealing with corporate crime. First, they found that enforcement efforts directed at the business organization act as a powerful deterrent for those who make decisions within the organization. Second, they found that enforcement efforts that are directly targeted at the individual decision maker also serve as an effective deterrent to corporate crime. Hence, threats of criminal and civil sanctions directed against the individual inhibited the

intention to commit corporate crime as well as the fear of informal sanctions. Third, the researchers found evidence to suggest that moral appeals may be an especially powerful source of corporate social control. As a result, strengthening the business ethics of corporate managers may prove to be a very effective crime-control strategy since moral inhibitions were found to be a very strong safeguard against corporate crime.

Based on their research findings, Paternoster and Simpson (1996) argued for a multifaceted approach to crime control. The researchers related that one part of this approach would be the moral education of those engaged in business. They also argued for a legalistic approach to corporate crime control through the enforcement of business laws and regulations. The researchers claimed that an appeal to legal sanction is necessary because findings indicated that an appeal to morality does not work for everyone. Therefore, when morality weakens, legal threats must be used to secure compliance. In addition, the threat of legal sanctions may be necessary to maintain the legitimacy of an extensive network of informal and normative controls. The researchers found that legal sanctions directed at the organization are a significant factor in supporting employees' beliefs that corporate crime is wrong, shame occurs if one were to commit it, and in strengthening the credibility of legal sanctions for employees. The researchers contended that theoretical models of corporate crime and public policy efforts must contain instrumental (threats of punishment) and deontological (appeals to morality) factors.

Vance and Siponen's rational choice model. In order to better understand the effect of expected benefits on IS security violations, Vance and Siponen (2012) used

Paternoster and Simpson's (1996) rational choice model as the basis for their theoretical model. Vance and Siponen reported that RCT had not been used in the field of IS. The researchers related that RCT explains individuals' decisions to commit crimes as utilitarian calculations based on perceived benefits and both formal and informal sanctions. Therefore, RCT extends beyond deterrence theory by including individuals' perceptions of benefits of violations and informal sanctions, and espoused moral beliefs. They noted that RCT is commonly used to explain criminal behavior; however, it is general enough to cover all violations. Vance and Siponen noted that RCT is also applicable to the study of violations of organizational IS security policies. The researchers also noted that RCT has been found to explain white-collar crimes better than street-level crimes. Due to this and because RCT has been found to be effective in the corporate context (e.g., Paternoster & Simpsons, 1996), Vance and Siponen related that they expected it to be a good fit for explaining intentional IS security policy violations, which also includes a deliberate violation of organizational norms.

To better explain IS security policy violations in situations where employees are aware of the IS security policy, Vance and Siponen's (2012) theoretical model includes disincentives (sanctions) and incentives (perceived benefits) for violating IS security policies. In addition, their model includes both informal sanctions, which are unstated social penalties; formal sanctions, which are explicit penalties for specific forms of misconduct; and moral beliefs. The researchers' RCT model includes formal sanctions, informal sanctions, moral beliefs, and perceived benefits.

In regard to formal sanctions, which are explicit penalties imposed for specific forms of misconduct, researchers found that the severity of the formal sanctions had a significant effect on users' intentions to commit computer abuses (e.g., D'Arcy, Hovav, & Galletta, 2009; Straub, 1990). Due to this theoretical and empirical support, Vance and Siponen (2012) hypothesized that "formal sanctions negatively affect intention to violate IS security policy" (p. 25). Examples of informal sanctions (unstated social penalties for undesirable behavior), include disapproval from friends or peers, social censure, or embarrassment (Bachman, Paternoster, & Ward, 1992; Grasmick & Bursik, 1990; Paternoster & Simpson, 1996). Vance and Siponen reported that depending on the type of offense, empirical findings regarding the effects of informal sanctions have been mixed. Therefore, the researchers hypothesized that "informal sanctions negatively affect intention to violate IS security policy" (p. 25).

Moral belief is another element of Vance and Siponen's (2012) rational choice model. Bachman, Paternoster, and Ward (1992) suggested that the traditional views of RCT do not take into account the moral beliefs of individuals. Bachman et al. posited that individuals may refrain from offending not because they fear sanctions but because they evaluate the offense as morally wrong. The researchers discussed two possible reasons for this, which are as follows: (a) Individuals' moral beliefs are so strong that other factors are irrelevant and (b) when moral beliefs are not strongly held, formal sanctions are then needed. Of these two components, Paternoster and Simpson (1996) found that moral inhibitions are the strongest predictor of corporate crime, which is supported by other research findings (e.g., Bachman et al., 1992; Ellis & Simpson, 1995). Vance and

Siponen claimed that moral beliefs are relevant to the context of information security because choices generally pertaining to information security and choices specifically pertaining to security policies involve a moral component (see Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009; Stahl, 2004). Vance and Siponen hypothesized that "moral beliefs negatively affect intention to violate IS security policy" (p. 26).

Findings from empirical studies have supported the notion that perceived benefits positively affect decisions to commit violations (e.g., Ducan, Lafree, & Piquero, 2005; Puhakainen, 2006; Wood, Gove, Wilson, & Cochran, 1997). Perceived benefits might be intrinsic such as the excitement some individuals may experience when committing a crime or extrinsic such as money (Ducan, Lafree, & Piquero, 2005; Puhakainen, 2006; Wood, Gove, Wilson, & Cochran, 1997). Puhakainen (2006) found that time saving is a major incentive to violate or avoid IS security policies. Vance and Siponen hypothesized that "perceived benefits positively affect intention to violate IS security policy" (p. 26).

To examine IS security policy violations, Vance and Siponen (2012) used a hypothetical scenario method. Data were collected from a high-tech services company and a major bank, both of which handled sensitive information. Both organizations were chosen because they used IS security policies and had clear sanctions in place for policy violations. Findings indicated that moral beliefs are an important predictor of intention to violate IS security policies, which is consistent with findings from previous research (e.g., Bachman et al., 1992; D'Archy et al., 2009; Elis & Simpson, 1995; Paternoster & Simpson, 1996; Siponen, 2000, 2002). Vance and Siponen's interpretation of this finding is that if employees view violations of IS security policies as morally wrong, they are less

likely to commit them. On the other hand, if employees believe that it is morally acceptable to violate the norm, then they are more likely to do so.

A second finding in Vance and Siponen's (2012) study indicated that perceived benefits also had a significant positive effect on intention, but the direction was opposite that of moral beliefs. Based on this finding, the researchers suggested that if employees see a benefit in violating IS security policy, then they are more likely to do so. As a result, they noted that mangers should take into account potential benefits that may prompt noncompliance, such as saving time. Thus, security managers may use IS security training to address the potential benefit of saving time, which may be perceived as a reason for policy violations.

A third finding was that the effect of formal sanctions was not supported (Vance & Siponen, 2012). Vance and Siponen (2012) noted that research pertaining to sanctions in the IS field are mixed. For example, D'Arcy et al. (2009) found that only the severity of formal sanctions effectively reduced IS misuse. In contrast, Hu, Xu, Dinev, and Ling (2010) found that formal sanctions had a small effect on employee intentions to commit computer offenses. A fourth finding was that the effect of informal sanctions was not supported; however, a small, significant effect ($p < .10$) was detected (Xu et al., 2010. 30). In regard to the interpretation of the formal sanctions and informal sanctions findings, the researchers argued that formal sanctions such as penalties and informal sanctions such as the loss of respect from management and coworkers, do not work as deterrents in the context of employees' compliance with IS security procedures. In regard to informal sanctions, the researchers related that employees do not care about penalties

and the loss of respect because they perceive penalties and lack of respect to be minor issues. Vance and Siponen also noted another possible interpretation related to Kohlberg's (1976, 1984) cognitive theory of moral development, which suggests that only individuals who are in the initial stages of moral development are influenced by sanctions.

In summary, moral beliefs, perceived benefits, and informal sanctions showed significant effects in explaining employee IS security policy violations (Vance & Siponen, 2012). In contrast, the effect of formal sanctions was insignificant (Vance & Siponen, 2012). Based on their findings, Vance and Siponen (2012) suggested that organizations should include other means to discourage IS security violations apart from formal sanctions because they are not always effective in deterring policy violations. Hence, in addition to formal sanctions, the researchers recommended that security managers engage in positive means of reinforcement, such as arranging IS security training sessions in order to persuade employees that the violation of IS security policies is morally wrong and compliance with policies is morally right. In regard to perceived benefits of violating IS security policies, the researchers suggested that top management and supervisors communicate clear and consistent message that saving work time does not justify the violation of IS security policies. Thus, adhering to IS security policies is important to employee job descriptions and responsibilities.

Research application of rational choice theory. Along with the benefits associated with the use of Internet technology in the workplace, threats such as increased security risks and improper use are major concerns for most companies (Li et al., 2010).

Li et al. (2010) reported that nonwork-related Internet activities, such as checking personal e-mails, browsing nonwork-related websites, chatting online, gaming, investing, shopping, and cybercrimes, reduces employees' productivity and can cause various security breaches such as viruses and spyware. Despite companies adopting and implementing Internet use policies (IUPs) to reduce employees' Internet misuse, the scope of Internet misuse is still on the rise due to noncompliance (Foster, 2006). Young and Case (2004) found that of the 25 companies that implemented IUPs, 40% found the policies to be an effective deterrent to curb employee Internet abuse, 40% did not find the policies effective, and 20% did not respond (p. 108). Of the 10 companies that used management training, 40% found it to be an effective deterrent, while 50% found it ineffective, and 10% did not respond (Young & Case, 2004, p. 108). Rehabilitation training was found to be effective by one company that used it as a way to deal with employee Internet abuse.

Prior to 2010, there was a lack of studies that provided full insight into why noncompliance with security policies occur because researchers ignored the effect of perceived benefits of deviant behaviors, moral values, and the conditions for formal sanctions to be effective (Li et al., 2010). As a result, Li et al. (2010) reported that they applied Paternoster and Simpson's (1996) rational choice model of corporate crime to examine how employees' intention to comply with IUP is driven by cost-benefit assessments, personal norms, and organizational context factors. Li et al. examined their research model, where they suggested that employees' IUP compliance intention will increase when (a) "employees perceive high threats from formal or informal sanctions or

high security risks to their computer or data and (b) employees have high personal norms against Internet abuses" (p. 637). In addition, based on their model, personal norms against Internet abuses can be increased by the joint effect of organizational norms and organizational identification.

Participants in Li et al. (2010) study were organizational employees and 246 usable responses were received from the online survey (p. 639). Li et al. (2010) reported that their findings were consistent with Paternoster and Simpson's (1996) rational choice model of corporate crime. Findings indicated that employees' intention to comply with the IUP involves a cost-benefit analysis. The researchers found that employees were more likely to comply with the IUP when perceived benefits were overridden by potential risks from formal sanctions and security threats. The deterrence effect of formal sanction risks was largely exerted through detection probability instead of sanction severity. Thus, sanction severity was not an effective deterrence mechanism for the majority of employees. In addition, the social influence from others who are important or subjective norms was not a significant predictor for the intention to comply with the IUP.

Furthermore, findings indicated that along with the cost-benefit analysis, compliance intention is also influenced by employees' personal norms or moral standards against Internet abuses (Li et al., 2010). Li et al. (2010) related that personal norms moderate the effect of perceived sanction severity on the compliance intention. Perceived sanction severity was found to be a significant deterrence mechanism only for employees with very low personal norms against Internet abuses. For employees with moderate to high personal norms, the perception of harsh sanctions failed to increase their compliance

intention and also reduced it. Harsh sanctions may undermine the trust or loyalty toward a company and create a counterproductive effect on the compliance intention among those with moderate to high personal norms against Internet abuses. In addition, the researchers found that organizational context factors could indirectly influence individual employees' compliance intention. Overall, results indicated that employees' compliance intention was the result of competing influences of perceived benefits, formal sanctions, and security risks. Moreover, the effect of sanction severity was found to be moderated by personal norms.

Findings from Li et al. (2010) study also indicated that employees conduct Internet abuses due to the perceived benefits, such as a more interesting work life. Li et al. (2010) noted that it may not be possible to use a zero Internet usage policy for personal purposes in the workplace as it could decrease employees' trust and morale and increase enforcement cost. Instead, the researchers recommended the use of a fair IUP with a clause that says "reasonable use" (p. 644). The researchers also recommended that companies use several approaches to ensure employees' IUP compliance. Thus, companies could increase personal moral norms against Internet abuses by cultivating voluntary compliance with security policies. Companies could further promote voluntary policy compliance though periodic security training, educating employees about risks from Internet security breaches. Companies could also implement various control mechanisms to monitor the usage of the Internet and inform employees that they could be caught if they abuse their Internet access. Hence, the sanction-based mechanism could be used to complement the voluntary compliance approach. Furthermore, the researchers

noted that companies could work to increase employees' organizational identification or their sense of belonging to the company so that employees are more likely to act in the company's interest and follow the IUP.

Social Learning Theory

In this subsection, I discussed the theoretical propositions of Bandura's (1974, 1977, 1986) SLT. In addition, I discussed how the theory has been applied previously in ways similar to this study. This subsection is organized in the following areas: theory and research application of social learning theory.

Theory. Bandura (1974, 1977, 1986) developed SLT in the 1960s, which was later changed to SCT in 1986 (Boston University School of Public Health, 2013). According to Boston University School of Public Health (2013), SLT posits that learning occurs in a social context with a three-way, dynamic and reciprocal interaction of the person, environment, and behavior. In this theory, focus is placed on social influence and external and internal social reinforcement. In SLT, consideration is placed on the unique way in which individuals acquire and maintain behavior, while considering the social environment in which individuals perform the behavior. The theory takes into account individuals' past experiences, which influences reinforcement, expectations, and expectancies. All of these factors shape whether individuals will engage in a specific behavior and the reasons for doing so.

SLT's goal is to explain how individuals regulate their behavior through control and reinforcement to achieve goal-directed behavior that can be maintained over time (Boston University School of Public Health, 2013). Boston University School of Public

Health (2013, para. 3) discussed six constructs, where Bandura developed the first five as part of SLT and the sixth construct known as self-efficacy was added when the theory evolved into SCT:

1. Reciprocal determinism: This is the theory's central construct and pertains to the dynamic and reciprocal interaction of person (an individual with a set of learned experiences), environment (external social context), and behavior (responses to stimuli to achieve goals).
2. Behavioral capability: This construct pertains to individuals' ability to perform a behavior through essential knowledge and skills. They learn from the consequences of their behavior, which affects their environment.
3. Observational learning: In regard to this construct, individuals can witness and observe a behavior that is conducted by others and then reproduce those actions; thus, modeling the behavior.
4. Reinforcements: This construct has the greatest ties to the reciprocal relationship between behavior and environment. It pertains to the internal or external responses of people's behaviors that affect whether they will continue or discontinue the behavior. Individuals may self-initiate the reinforcement or it may be from the environment, which may also be positive or negative.
5. Expectations: This pertains to the anticipated consequences of individuals' behaviors. Individuals anticipate the consequences of their actions before they engage in the behavior and these anticipated consequence influence the successful completion of the behavior.

6. Self-efficacy: This construct is influenced by individuals' confidence in their ability to successful perform a behavior. Self-efficacy is influenced by people's specific capabilities, other individual factors, and environmental factors such as barriers and facilitators.

Therefore, in contrast to other learning theories, SLT emphasizes reciprocal relationship between social characteristics of the environment, how individuals perceive them, and how motivated and able individuals are to reproduce behaviors they see occurring around them (Health Communication Capacity Collaboration, 2015). In summary, Health Communication Capacity Collaboration (2015) related that in regard to SLT, people learn by observing what others do, consider the consequences that others experienced, rehearse (mentally first) what might happen in their own lives if they followed other's behavior, take action by trying the behavior, compare their experiences with what happened to others, and confirm their belief in the new behavior.

Research application of social learning theory. The relationship between deterrence and SLT has been discussed on numerous occasions by Akers (1977, 1985, 1990). According to Akers (1990), empirical tests of SLT have included measures of both formal deterrence (perceived probability of being caught by police officers) and informal parental deterrence (perceived probability of being caught by parents). Akers noted that the term deterrence is used because the measures referred only to perception of the likelihood of punishment. The author noted that neither formal deterrence nor informal parental deterrence have much direct effect because each pertain to variation in perceived likelihood of aversive consequences. Therefore, other variables that measure both reward

and aversive consequences and the balance of positive and negative reactions from peers and parents have strong effects. The behavioral formula in SLT includes both positive and negative punishment and reinforcement. In addition, it includes schedules of reinforcement, imitation, associations, normative definitions such as attitudes and rationalization, discriminative stimuli, and other variables in criminal and conforming behavior.

Using SLT as their theoretical foundation, Yiu, Xu, and Wan (2014) extended corporate financial fraud research by developing a new perspective on the deterrence effects of vicarious punishments. The researchers posited that employees vicariously learn about punishments from their peers by picking up modeling cues, environmental cues, and social cues in the inhibitive learning process; thus, becoming deterred from committing future fraudulent acts. The researchers used a matched sample of 604 listed companies between 2002 and 2008. Findings showed that an observing employee was deterred from committing fraud if peers in the industry were caught and punished. Furthermore, such deterrence effects are dependent on how observing employees evaluate the possibility of being caught and the likelihood that they will be similarly punished if they violate similar prohibitions. In particular, the researchers found that inhibitive learning effects were positively moderated by punishments of prominent employees and model-observer similarity but negatively attenuated by the development of the legal system. The researchers' study illuminated the indirect, inhibitive learning process from vicarious punishments and identified the conditions for differential learning and deterrence outcomes of the observing employees.

Background of Polygraph Testing

Advancements in medical understanding of human physiology and advances in the field of psychology led to combining a number of measurable physiological reactions on a single sheet of paper, which became known as the polygraph (Kleinmuntz & Szucko, 2004). The term polygraph originally meant *many writings* but now represents a specific field that operates at the confluence of psychology and human physiology (American Polygraph Association, 2013; National Research Council, 2003; Nelson, 2015). According to the NCCA (2013b), the term most commonly applied to polygraph is *psychophysiological detection of deception*. The term polygraph originated with the multiple physiological reactions recorded on a single medium. Originally the medium was paper, but with the introduction of computers, a file with graphically represented physiology similar to what would be recorded on paper, along with other pertinent file details, is now standard (Handler & Nelson, 2015; NCCA, 2013b).

Marston and Reid were significant figures in the evolution of the polygraph test and expanded the use of polygraph testing within the federal government (Bunn, 1997; National Research Council, 2003). Marston developed interview and physiology collection techniques (Bunn, 1997; National Research Council, 2003). Specifically, Marston invented the discontinuous polygraph, which records physiological signals only at select times during an interrogation (Sylvers & Lilienfeld, 2015). Sylvers and Lilienfeld (2015) reported that Moulton claimed that the polygraph was the solution to detecting deception during interrogation. The researchers noted that in 1921, Larson built on Marston's invention and created the continuous polygraph called cardio-pneumo-

psychograph. However, in contrast to Marston, Larson was critical of the polygraph and cautioned against its use in court proceedings. In line with Larson's viewpoint, the U.S. Supreme Court decided in *Frye v. United States* (1923) that there was insufficient scientific support to allow polygraph results to be used as evidence in court proceedings.

In response to the *Frye* ruling, scientists worked towards developing scientifically validated polygraph techniques (Sylvers & Lilienfeld, 2015). In 1930, Larson's associate, Keeler, and Reid who was a major proponent of law enforcement's use of polygraph testing, assisted in forming the Scientific Crime Detection Laboratory of Northwestern University (Bunn, 1997; National Research Council, 2003; Sylvers & Lilienfeld, 2015). In 1938, Keeler opened the first polygraph training school and in 1947, Reid opened John E. Reid and Associates (Sylvers & Lilienfeld, 2015). These two schools became the most prominent U.S. polygraphy schools (Sylvers & Lilienfeld, 2015).

Although most polygraphs measure similar physiological indicators, polygraphers use different interrogation techniques (Sylvers & Lilienfeld, 2015). Sylvers and Lilienfeld (2015) related that the three most commonly used methods of interrogation are the irrelevant/relevant (I/R) test, the control question test (CQT), and the guilty knowledge test (GKT). The researchers noted that the I/R test was the original method of interrogation and this method is still commonly used by employers during personnel screening interviews. Sylvers and Lilienfeld reported that the I/R test uses a combination of task-irrelevant and task-relevant questions. The CQT is a variant of the I/R test and is currently the method that is most commonly used in the United States (Sylvers & Lilienfeld, 2015). Sylvers and Lilienfeld noted that this method uses a combination of

control, task-relevant, and task-irrelevant questions. The GKT technique is used to investigate criminal guilt without attempting to identify a lie response; therefore, it is a sharp contrast from the I/R test and CQT. Polygraphers use the GKT to assess concealing knowledge by asking specific questions about the crime followed by multiple choice options. The researchers noted that U.S. law enforcement agencies rarely use the GKT.

The polygraph examination generally relies on a structured interview, a thorough review of questions to be asked, a collection of physiological responses to those questions in a structured format, and if necessary, a postexamination interview (American Polygraph Association, 2013; Nelson, 2015). There has been minimal change to the actual physiological collection aspect of polygraphy since the U.S. Government began using the polygraph as an investigative tool in the 1950s (American Polygraph Association, 2013; Nelson, 2015). The four general physiological channels that are recorded are breathing, cardio activity, electrodermal conductance, and movement (American Polygraph Association, 2013; Handler & Nelson, 2015; Nelson, 2015). A structured series of questions are asked, which are recorded on a computer, and the examiner evaluates the physiological reactions to the various questions (American Polygraph Association, 2013; Handler & Nelson, 2015; Nelson, 2015)..

The methods used in polygraphy have been extensively researched similar to other commonly accepted forensic investigative techniques, such as hand writing analysis, witness line-ups, and crime scene evidence collection (Cochrane, Tett, & Vandecreek, 2003; National Research Council, 2003). Currently, polygraph examinations are mainly used in law enforcement and the U.S. Intelligence Community (Executive

Branch, 2008; NCCA, 2011; National Research Council, 2003; ODNI, 2015a). The major uses for the polygraph exam in the U.S. are for pre-employment screening, sensitive program access screening for current employees, and specific issue exams for resolving issues such as crimes (DOD, 1984; Handler & Nelson, 2015; ODNI, 2015a). Reliability rates vary depending on whether or not the exam is a multiple issue exam or a specific issue exam (DOD, 1984; Handler & Nelson, 2015; ODNI, 2015a). Resolution rates, when inconclusive calls are excluded, are well over chance, often approaching 85% to 95% or higher when a conclusive result is reached (Gougler et al., 2011; Nelson, 2015).

Employee Polygraph Protection Act of 1988

Until the late 1980s, many American businesses used polygraph testing as a tool to screen job applicants and employees (Sylvers & Lilienfeld, 2015). However, with the passage of the EPPA of 1988, which is enforced by the DOL, employers engaged in interstate commerce are not permitted to use lie detector tests for preemployment screening or during the course of employment, with certain exemptions (American Polygraph Association, 2005; Sylvers & Lilienfeld, 2015; DOL, 2008). According to the DOL (2008), exempt from the Act are federal, state, and local governments (DOL, 2008). The federal government is permitted to give lie detector tests to employees of federal contractors engaged in national security intelligence or counterintelligence functions. The polygraph, but no other lie detector tests, may be administered in the private sector for the following reasons (DOL, 2008, para. 6):

1. To employees who are reasonably suspected of being involved in a workplace incident that results in economic loss to the employer and who had access to the property that is the subject of the investigation.
2. To prospective employees of armored car, security alarm, and security guard firms who protect facilities, materials, or operations affecting health or safety, national security, or currency and similar instruments.
3. To prospective employees of pharmaceutical and other firms authorized to manufacture, distribute, or dispense controlled substances who will have direct access to such controlled substances. In addition, to current employees who had access to persons or property that are the subject of an ongoing investigation.

Examiners are required to have a valid or current license if it is a prerequisite by the state in which the polygraph test is to be conducted (DOL, 2008). The DOL (2008, para. 7) also noted that examiners are required to maintain a minimum of $50,000 bond or professional liability coverage. Under the Act, prospective and current employees also have legal rights. For example, prospective and current employees must be given a written notice that explains their rights and the limitations imposed, such as questions that are prohibited and restrictions on how the test results can be used. Within 3 years of an alleged violation, prospective and current employees also have the right to take civil actions in a federal or state court against employers who violate the Act for legal or equitable relief, such as job reinstatement, promotion, and payment of loss wages and benefits.

Polygraph as a Deterrent Against Security Compromises

In an effort to address issues of crimes and screening for intelligence purposes, the U.S. Army instituted its own polygraph training academy in the early 1950s (NCCA, 2013b). Use of the polygraph expanded from the U.S. Army to the federal government and law enforcement agencies to use within the commercial sector (NCCA, 2013b). Some employees who worked as clerks and bank tellers also had to do polygraph testing (Kleinmuntz & Szucko, 2004). The expansive use of polygraph testing was driven by organizations' attempt to reduce theft of merchandise and money (National Research Council, 2003).

However, there were exceptions to the law, which allowed federal government and law enforcement agencies to require a polygraph as a condition of employment (DOD, 1984; DOL, 2013; U.S. Government, 2013). The U.S. Army, a uniformed service within the DOD, is authorized to use a screening polygraph to enhance protection of its programs and seek out violations of certain national security laws (DOD, 1984; U.S. Army, 1995; U.S. Government, 2013). The Intelligence and Security Command of the U.S. Army, a member of the Intelligence Community, is authorized to use screening polygraph examinations as part of its employee vetting process (DOD, 1984; U.S. Army, 1995; U.S. Government, 2013). One of the purposes of requiring individuals to undergo these screening exams is to protect programs that are attractive targets for foreign governments, terrorist groups, and insider threats (DOE, 2013). One of the stated goals of the U.S. Army Intelligence and Security Command's polygraph program is to deter intentional violations of applicable security regulations (U.S. Army, 1993). However,

despite deterrence efforts taken by many federal-level organizations, such as the U.S. Army's use of polygraph testing, some organizations fall victim to deliberate security compromises (Defense Personnel and Security Research Center [PERSEREC], 2009; Executive Branch, 2008).

The ODNI is an organization created in the wake of the September 11, 2001 terrorist attacks (9/11) to integrate foreign, military, and domestic intelligence in defense of the United States (ODNI, 2013). There are 17 members of the U.S. Intelligence Community and the ODNI is charged with providing direction and deconfliction to each member on a national level (ODNI, 2013, 2015b). The U.S. Army's Intelligence and Security Command falls under the Army Deputy Chief of Staff for Intelligence and is a member of the U.S. Intelligence Community (ODNI, 2015b).

Despite the use of polygraph analysis, a number of other high profile information leaks have occurred of sensitive operations such as the foiling of a covert al-Qa'ida plot to blow up an airliner with a sophisticated undergarment bomb, a collaboration of U.S. and Israeli cyber operations designed to disrupt Iranian nuclear ambitions, and supposed release of unauthorized information to journalists about the covert raid to kill Osama bin Laden (Mak, 2012). This problem has become increasingly more political. To help protect high level national security information, Clapper, the Director of National Intelligence, announced steps to detect and deter unauthorized disclosures (ODNI, 2012). The ODNI (2012) reported that these steps included the addition of a mandated question in relation to unauthorized disclosure of classified information to the counterintelligence polygraph. The director announced the independent investigations of selected

unauthorized cases by the intelligence community inspector general (ICIG) when Department of Justice (DOJ) declines to prosecute. The goal is to prevent selected unauthorized disclosures cases that meet the threshold for administrative investigation from being prematurely closed.

Polygraph's Effect on Employees' Behaviors and Attitudes

Polygraph examinations are used for preemployment or preclearance screening in agencies involved in national security (National Research Council, 2003). The National Research Council (2003) noted that current employees who are being considered for new assignments, normally at a higher level of clearance, take part in preclearance screening. Insider threats are becoming more frequent due to a number of reason, such as the following (Figliuzzi, 2012, para. 4):

1. The pervasiveness of employee financial hardships during economic difficulties.
2. The global crisis facing foreign nations, which makes it even more attractive.
3. Cost-effective and worth the risk to steal technology rather than invest in research and development.
4. The ease of stealing anything stored electronically, especially when the individual has legitimate access to it.
5. The increasing exposure to foreign intelligence services presented by the reality of global business, joint ventures, and the growing international footprint of U.S. companies.

The U.S. Army's Intelligence and Security Command uses the polygraph in the

execution of its intelligence mission (U.S. Army, 1993, 1995; U.S. Government, 2013). Among the mission of the polygraph program is deterrence of national security crimes such as deliberate mishandling of classified information, espionage, and terrorism (DOE, 2013; U.S. Army, 1993). In order for a deterrence to be effective, researchers mentioned that the population that is expected to change should be aware that there are certain consequences (e.g., Nagin & Paternoster, 1991; Nagin & Pogarsky, 2003; Paternoster et al., 1983a; Watson, 1986). Similarly, Wright (2010) noted that employees who leak information should be aware that there is an increased likelihood of detection and subsequent punishment. The National Research Council (2003) noted that individuals who are subjected to polygraph testing will either resign to avoid the exam and subsequent interrogation, decide not to engage in a prohibited behavior, or simply avoid a particular agency altogether. For those subjected to polygraph testing on a regular basis in order to gain continued access to sensitive programs, the desired effect is that of continued adherence to rules, or self-directed behavior and attitude change, or modification (Nagin & Paternoster, 1994; Nagin & Pepper, 2012; ODNI, 2015a; U.S. Army, 1993).

An example of this can be seen with the U.S. Navy drug testing program. Drug testing has affected the U.S. Navy in a dramatic way. After the U.S. Navy instituted mandatory and random drug testing for its personnel in 1981, the U.S. Navy saw an immediate drop of 60% in drug use (Borack, 1998). Researchers found that the drop was attributed to the deterrence effect of personnel avoiding or changing their behavior (Borack, 1998; Peterson, Jung, & Stanley, 2008; Strelan & Boeckman, 2006).

Adhering to Security Regulations Due to Polygraph

The use of polygraph has been mandated for employees in certain jobs who have access to highly sensitive information and activities in an effort to deter leaks (U.S. Army, 1993). The use of polygraph testing as a deterrence in the national security setting focuses on reducing incidents of espionage, sabotage, terrorism, unauthorized foreign contact, and deliberate mishandling of classified information by expectations of changes in behavior and attitude (DOE, 2013; U.S. Army, 1993). During a screening examination, one of the national security issues that is tested for is the mishandling of classified information (National Research Council, 2003; ODNI, 2012). Pozen (2013) noted that security compromises of classified information are very difficult to prosecute. Even though there have been over 100 successful prosecutions for espionage, there are probably hundreds of security compromises of classified information every year to the media (PERSEREC, 2009; Pozen, 2013). Pozen argued that historically, there has been a level of complacency within the Executive Branch in prosecuting security compromises.

Security compromises are a type of informal currency through which one can gain an advantage (Pozen, 2013). Pozen related that it is also a very secretive world in which journalists protect confidential informants to the point of voluntarily going to jail to protect their identity (Pozen, 2013; Schmitt, 2005). An example of a major security compromise involves Private First Class Bradley Manning who leaked the U.S State Department's cables and Iraq war logs (U.S. Army, 2011; *United States v. Manning*, 2013). Manning leaked hundreds of thousands of classified U.S. State Department cables to Wikileaks, an organization dedicated to whistle blowers anonymity, who subsequently

published most of the documents on the Internet (U.S. Army, 2011; *United States v. Manning*, 2013). In contrast to high ranking members of the executive branch who are most often associated with leaks, Manning was a low-level U.S. Army intelligence analyst (Elsea, 2013; Pozen, 2013; U.S. Army, 2011; *United States v. Manning*, 2013). Similarly, there are a number of incidents in which former CIA employees accidentally or intentionally released information about classified operations or undercover agents (Associated Press, 2013; Liptak, 2005; Mak, 2012).

Convicted Russian espionage agent and former U.S. Naval Warrant Officer John Walker was instructed by his Russian case officers to avoid attaining a job that required a polygraph in order to continue his access to classified information without increased fear of detection (PERSEREC, 2009). The PERSEREEC (2009) reported that Walker was instructed to retire instead of being promoted into a job that required a polygraph. Similarly, convicted spy and former FBI agent Robert Hanssen also avoided jobs where polygraph exams were required as a condition of employment. The PERSEREEC further related that the CIA uses polygraph exams to maintain security, to include counterintelligence investigations that rooted out and provided evidence to prosecute Russian Spy Harold Nicholson. Other successful national security crime prosecutions that were predicated on polygraph admissions include those by former U.S. Navy Seaman Steven Hawkins, who admitted to storing classified documents with plans to sell them to a foreign government in 1981; Steven Lalas, imprisoned for espionage on behalf of Greece and admitted much more than initial debriefings indicated only after failing a number of polygraph exams in 1993; and Ronald Montaperto, convicted of espionage for

China and made full disclosure of espionage only after being confronted during a polygraph session in 2003 (PERSEREC,, 2009).

After a series of high profile security compromises, President Obama ordered Clapper, Director of National Intelligence, to coordinate and conduct more comprehensive polygraph exams in an attempt to root out unauthorized disclosures, calling it a *war on leakers* (Mak, 2012; ODNI, 2012; Pozen, 2013). Pozen (2013) related that while the federal government has the right to pursue prosecution against those who are suspected of leaking information, the courts generally protect the press. The Obama Administration is responsible for half of the prosecutions pertaining to leaked information to the press since the Espionage Act of 1917 (DOJ Office of Public Affairs, 2012; Mak, 2012; Schmidt, 2013; Schmitt, 2005). Pozen highlighted that there are few successful prosecutions despite the huge number of leaks. However, the Obama Administration attained a guilty plea in the prosecution of a former CIA employee who provided details about covert operations and sources to a member of the media. The former employee plead guilty to disclosing the identity of an undercover agent. This successful prosecution of the former CIA employee has emboldened the Obama Administration as they have added additional charges against other individuals awaiting prosecution for security violations (Aftergood, 2012; *United States of America v. Hitselberger*, 2012).

Summary and Conclusions

Since recorded history, mankind has sought ways of determining if another person is being deceptive (National Research Council, 2003). With scientific developments and

improvements in law enforcement, a method known as polygraph analysis was developed to record changes in physiology which resulted in a high resolution rate in detecting certain types of deception (National Research Council, 2003). This technique was eventually refined and adapted by the DOD, who now uses it in an effort to deter and detect certain types of national security crimes (DOD, 1984; DOE, 2013; Handler & Nelson, 2015; NCCA, 2011).

Deterrence results in either behavior and attitude change that are more consistent with the organization or a person avoids employment at an agency that requires a screening polygraph (National Research Council, 2003). Wright (2010) noted that in order for deterrence to be effective, the population where the deterrence effect is sought must be aware of both severity and certainty of a punishment. Even though severity has an effect on deterrence, the certainty of detection and punishment has a much greater effect (Nagin & Paternoster, 1991; Nagin & Pogarsky, 2001; Paternoster et al., 1983b; Wright, 2010). For example, the change in behavior and attitude when there is certainty of punishment can be seen in the changes in drug use within organizations that mandate both initial and random drug testing for its employees (Borack, 1998). In the U.S. Navy, there was a 60% decrease in drug use in the early 1980s when it instituted mandatory drug testing for its employees (Borack, 1998, p. 17).

Similar to drug testing, random polygraph testing to ensure compliance with regulations, has shown significant effects when individuals understand that there is an increased chance of detection and sanction (Borack, 1998; Strelan & Boeckman, 2006). Researchers noted that deterrence can be effective by increasing the number of random

tests on a larger population, as opposed to the mandatory testing of a large population (Abrams & Abrams, 1993; Apel, 2013; Nagin & Paternoster, 1994; Nagin & Pogarsky, 2003). The fear of detection of a crime is enough to cause social change because individuals may be subjected to a polygraph test (Paternoster et al., 1983a; Watson, 1986; Weisburd Waring, & Chayet, 1995).

Polygraph testing is often used to detect the mishandling of classified information (Pozen, 2013). The Obama Administration directed the Director of National Intelligence to increase its review of polygraph questions concerning the mishandling of classified and placed an emphasis on leaks to the media (ODNI, 2012, 2015a). The goal is to deter and detect unauthorized disclosures (ODNI, 2012).

For polygraph to be an effective deterrent, employees must be aware of its use, its effectiveness, and the certainty of crime detection (Nagin & Paternoster, 1994; Nagin & Pepper, 2012; Nagin & Pogarsky, 2001, 2003; Paternoster et al., 1983b). Pozen (2013) noted the historical failure of the Executive Branch to pursue leakers, despite statutes that allow for their prosecution. The author reported that leakers within the Executive and Legislative Branches are responsible for the vast majority of leaks. Research on criminal deterrence indicated that certainty of detection has a much greater deterrent effect on employees (Nagin & Paternoster, 1991, 1994; Nagin & Pogarsky, 2001; Paternoster et al., 1983a). Other deterrent factors include individuals' state of mind and their moral compass (Strelan & Boeckman, 2006).

Paternoster and Simpson's (1996) rational choice model of corporate crime, Vance and Siponen's (2012) rational choice model, and Bandura's (1974, 1977, 1986)

SLT were used as the theoretical foundation in this study. While insider threats may be maliciously intended, some are attributed to negligence or ignorance of security polices (Herath & Rao, 2009). Herath and Rao (2009) found that employees' perceptions about the severity of breach, response efficacy, and self-efficacy tend to have a positive effect on attitudes towards security policies. The researchers also found that social influence had a significant effect on compliance intentions and resource availability was a significant factor in increasing self-efficacy. Self-efficacy was found to be a significant predictor of policy compliance intentions. Employees' organizational commitment played two roles by impacting intentions directly and promoted a belief that employee actions have an effect on an organization's overall information security.

In Chapter 2, I included the introduction, literature search strategy, theoretical foundation, background of polygraph testing, Employee Polygraph Protection Act of 1988, polygraph as a deterrent against security compromises, polygraph's effect on employees' behavior and attitudes, adhering to security regulations due to polygraph, and a summary and conclusions. In Chapter 3, I include the introduction, research design and rationale, methodology, data analysis plan, threats to validity, and a summary. In Chapter 4, I include the introduction, pilot study, data collection and study results, and a summary of the chapter. In Chapter 5, I include the introduction, interpretation of findings, limitations of the study, recommendations, implications, and a conclusion to the study.

Chapter 3: Research Method

Introduction

The purpose of this descriptive and exploratory research study was to determine whether there was a perceived deterrence effect related to the use of polygraphs between a group of participants who were subjected to a polygraph examination within the past year compared to those who either had never experienced a polygraph or the experience was more than a year prior to the distribution of the survey. I used a 15-minute researcher-developed questionnaire. Cluster sampling was used to select the sample of 152 polygraph-treatment group and 174 no polygraph-treatment group (N = 326).

Data analysis included t test and factor analysis. Data was analyzed using SPSS. The study was conducted in accordance with Walden University's Institutional Review Board (IRB) guidelines to ensure the ethical protection of research participants. The IRB approved the application for the study and the approval number is 08-13-14-0118381. In Chapter 3, I include the research design and rationale, methodology, data analysis plan, threats to validity, and a summary of the chapter.

Research Design and Rationale

A descriptive and exploratory research design was used. This research design was appropriate as the goal of the research study was to determine whether there was a statistically significant difference between the polygraph-treatment and no polygraph-treatment groups' perceptions of the deterrence effect of polygraph examinations. McNabb (2008) pointed out that descriptive studies "provide a description of an event or define a set of attitudes, opinions, or behaviors that are observed or measured at a given

time and environment" (p. 97). Participants in the polygraph-treatment group were employees who worked in the intelligence field and were subjected to random polygraph testing as part of their work. Specifically, I used participants who took a polygraph through the U.S. Army Intelligence Polygraph Program, which has offices in South Korea and Fort Meade, Maryland. Participants in the no polygraph-treatment group were individuals who have never experienced a polygraph or the experience was more than a year prior to the distribution of the survey. They were recruited from the local vicinity of where I lived and worked in South Korea, the Walden University participant pool, and from the Walden University online community site, LinkedIn.

The method of data collection was a survey. Data on the surveys were collected through a 5-point Likert scale. A Likert scale is useful for data collection where I essentially collected ordinal data, but needed to interpret them as though the data were interval or ratio level data. The scale's summative nature allows the individual perception of deterrent effects to be quantitatively displayed and compared to another group, and has been successfully used in past research on deterrence (Nagin & Pogarsky, 2003).

Researchers have found that increasing the certainty of detection of undesirable behaviors can have a deterrent effect on individuals engaging in those behaviors (Nagin & Pepper, 2012; Nagin & Pogarsky, 2001, 2003; Paternoster et al., 1983a). These researchers used a self-report method in their studies and noted the necessity of anonymity in exchange for truthfulness when assessing potential negative behaviors and attitudes, such as willingness to commit a crime in both the presence and absence of punishment and authority figures (Nagin & Pepper, 2012; Nagin & Pogarsky, 2001, 2003;

Paternoster et al., 1983a). Nagin and Pogarsky (2003) noted that summative scales or perceptual surveys allow participants to better express their concern for sanction of risks prior to offending.

The use of the Likert scale format was needed in this study in order to determine self-reported behavior and attitude changes. The Likert scale format allowed participants to express the likelihood of behavior and attitude change when exposed to a situation in which they are more likely to have violations of regulations detected through polygraph exams. Participants' perceptions were important in determining polygraph's deterrence effect against security compromises. Individuals with access to national security information and who are employed in law enforcement positions are briefed on a regular basis about their responsibilities in protecting national security and community standards, as well as the sanctions for failure to protect such information (National Research Council, 2003). Prior knowledge of potential sanctions increases deterrence since the rational actor can then consider risk versus gain (Nagin & Pogarsky, 2003). Nagin and Pogarsky (2003) noted that sanctions must be known in order for the deterrence effects to be felt within the population. Likewise, the researchers noted that individuals knowing the sanctions and that there is an increased likelihood of detection deters negative actions. Most screening polygraph examinees are aware of restrictions placed on their access to sensitive information prior to their polygraph examination.

Methodology

In this section, the methodology was discussed. Sufficient depth was provided so that other researchers can replicate the study. This section is organized in the following

subsections: population; sampling and sampling procedures; procedures for recruitment, participation, and data collection (primary data); pilot study; instrumentation; and variables.

Population

The sample consisted of 326 volunteer participants, all of whom were U.S. citizens or legal resident aliens located in South Korea and the United States. Demographics were not collected due to a guarantee of anonymity and demographics could have been used to identify likely volunteers. Originally, 372 individuals started the online survey, but 326 total completed the survey, with the no polygraph-treatment group having 174 participants and the polygraph-treatment group having 152 participants. The completion rate for the surveys once a participant had started was 88%.

The 152 participants in the polygraph-treatment group were individuals who had recently taken a screening polygraph examination within the previous year and were currently in a position that required a polygraph as part of their job. They had taken the polygraph through the U.S. Army Intelligence Polygraph Program, which has offices in South Korea and Fort Meade, Maryland. The 174 participants in the no polygraph-treatment group were individuals who had not taken a screening polygraph examination in the last year and who were not required to take a polygraph as part of their job requirements. I used nonintelligence personnel in the local vicinity where I lived and worked in South Korea. In addition, students from the Walden University participant pool were used, of which 56 students received credit for attempting to complete the surveys. I also recruited and used individuals from the Walden University online community site,

LinkedIn.

Sampling and Sampling Procedures

I conducted an independent cluster sampling from all participants. Cluster sampling refers to a sampling method that has the following properties: (a) the population is divided into *N* groups, called clusters; (b) the researcher randomly selects *n* clusters to include in the sample; (c) the number of observations within each cluster M_i is known, and $M = M_1 + M_2 + M_3 + ... + M_{N-1} + M_N$; and (d) each element of the population can be assigned to one, and only one, cluster (Stat Trek, 2015, para. 1). One cluster, the polygraph-treatment group, were individuals who had recently taken a screening polygraph examination within the previous year and were currently in a position that required a polygraph as part of their job. Annually, within the DOD, there are approximately 40,000 screening polygraph examinations conducted (DOD, 2009; National Research Council, 2003). There are, however, no openly available demographic or background data on individuals that typically receive a screening examination. Generally, polygraph offices are located within communities that have a high concentration of demand, such as placing a polygraph office near a large intelligence processing center or base (National Research Council, 2003). I am currently located in South Korea, so I recruited locally for both groups. I used the U.S. Army Intelligence Polygraph Program with offices in South Korea and Fort Meade, Maryland, as a source for the polygraph-treatment group.

I recruited approximately 170 volunteers for the second cluster, the no polygraph-treatment group. The second cluster of individuals were those who had not taken a

screening polygraph examination in the last year and who were not required to take a polygraph as part of their job requirements. Nonintelligence personnel were recruited from the local vicinity of where I lived and worked in South Korea, the Walden University participant pool, and the Walden University online community site, LinkedIn. The identities of individuals who participated in the study were not known due to anonymity attributed to the online survey. This sampling strategy was one of convenience due to the remote location of my work site at the time in South Korea.

G*Power 3.1.7 was used to assess the required sample size for an independent sample *t* test. Using a medium effect size ($d = 0.50$), a generally accepted power of .80 is recommended when doing a *t* test for means (Sawyer, 1982); thus, a power level of 0.8 was used, and an alpha level of .05, the required sample size is 128. For exploratory factor analysis in developing surveys, Field (2009) recommended at least 300 samples. Therefore, at least 300 (final results were $N = 326$) participants were needed to be used to have a large enough sample size to obtain significant findings.

Procedures for Recruitment, Participation, and Data Collection (Primary Data)

I completed the National Institutes of Health (NIH) Human Research Protections training prior to data collection. In addition, I complied with all U.S. federal and state regulations, which included informing participants about the level of confidentiality and anonymity in the study. I began data collection after receiving approval to conduct the study from the Walden University IRB.

I received permission to conduct the study from a polygraph branch chief in the U.S. Army Intelligence Polygraph Program. For the polygraph-treatment group, I

recruited individuals who completed a polygraph examination from both the South Korea and Fort Meade, Maryland locations. I gave a hard copy consent form with the link to the survey to individuals who had completed a polygraph tests within the past year. Permission was also obtained from the branch chief to allow colleagues who administered the polygraph at either location to provide individuals who had completed a polygraph within the last year a hard copy consent form with the link to the survey. The consent form outlined participants' anonymity in the study as there would be no way to identify who completed the survey (see Appendix A). The consent form outlined that no compensation was offered for their voluntary participation. The consent form also stated there were no connections between my study and their examination; therefore, they should not expect any preferential treatment as a result of their voluntary participation in the study. Individuals who had pending polygraph examinations with me were excluded from taking part in the study in order to prevent a possible conflict of interest or perceived quid pro quo bias.

For the no polygraph-treatment group, with the permission of program managers in the local vicinity where I lived and worked in South Korea, I recruited participants who did not require a polygraph test as part of their job requirement or individuals who did not complete a polygraph within more than a year prior to the distribution of the survey. In addition, students from the Walden University participant pool were recruited, of which 56 students received credit for attempting to complete the surveys. I also recruited and used individuals from the Walden University online community site, LinkedIn. Individuals under 18 years of age were excluded from participating in the

study.

All participants were given a hard copy consent form with the survey link. The consent form was also available on Survey Monkey. Implied consent was used; therefore, the study replied on implicit endorsement rather than signed endorsement as participants were informed on the consent form that completing the web link survey indicated their voluntary consent to take part in the study. Participants completed the survey on Survey Monkey (see Appendix B for the questionnaire). The Survey Monkey account was set to ensure complete anonymity so that I could not identify individuals based on their responses. In order to ensure anonymity, no demographic information was collected. An advantage to using Survey Monkey was that it automatically saved the data into a form compatible with the SPSS. The initial collection of the data determined if the individuals were assigned to the polygraph-treatment or no polygraph-treatment group. All nonattributable digital data from the questionnaires are kept on removable media in a safe accessible only to me for a period of 5 years.

Participants in the study may have access to the results now that the research is completed and approved. If participants want the results, they were instructed to send an e-mail request to me. My e-mail address was provided on the consent form. Due to the nature of the survey, it was unlikely that participation aroused any acute discomfort, such as psychological harm, economic loss, damage to professional reputation, and physical harm.

Pilot Study

The term, pilot studies, refer to mini versions of a full-scale study, which is also

called feasibility studies, as well as the specific pretesting of a particular research instrument such as a questionnaire or interview schedule (van Teijlingen & Hundley, 2001). Similarly, Leon, Davis, and Kraemer (2011) reported that the purpose of conducting a pilot study is to examine the feasibility of an approach that is intended to be used in a larger scale study. Pilot studies are used to improve the internal validity of a questionnaire (van Teijlingen & Hundley, 2001).

Prior to the main study, I conducted a pilot study to test the reliability and validity of the questions on the survey, as well as the feasibility of implementing the data collection methodology. I collected at least 25 surveys in each of the polygraph-treatment and no polygraph-treatment group (no polygraph-treatment $N = 56$; polygraph-treatment $N = 26$). Once the surveys were electronically completed, the data from the survey were automatically uploaded into SPSS for evaluation. The reliability of the survey was determined by the use of the split-half method. I also conducted an exploratory factor analysis to determine factors related to deterrence and ran a Cronbach's alpha to determine reliability of the questionnaire (Cronbach's alpha = >.90). The SPSS was used to display the descriptive statistics of the range, skew, and the standard deviation.

Instrumentation

The instrumentation for this study was a 15-minute researcher-developed questionnaire that was used to obtain the perceptions of participants about the perceived deterrence effect related to the use of polygraphs (see Appendix B). Researchers have used similar types of perception surveys in their investigation on deterrence (Nagin & Paternoster, 1991; Nagin & Pogarsky, 2001). The questionnaire was divided into two

distinctly different sections. The first section identified the participant's group (polygraph-treatment or no polygraph-treatment), and included the informed consent information. No demographic data were collected except for participants' polygraph experiences and whether or not their job required a polygraph. Therefore, no identifying data were collected. The second section of the survey contained the scaled questions along with definitions, which ensured a degree of consistency for certain terms used in the questions. A 5-point Likert scale format was used, ranging from 5 (strongly agree) to 1 (strongly disagree). Three items were reverse scored. The questions were developed to determine a participant's self-reported likelihood of behavior and attitude change and perceptions of polygraph's deterrence effects.

In developing the questions used in the survey, I received assistance from two agencies, the NCCA and the U.S. Army Intelligence Polygraph Program. To help establish the validity of the survey, a member of the research department of the NCCA and a retired polygraph examiner and former employee of the CIA also reviewed the survey questions and provided additional comments to the proposed questions to ensure consistency with community standards. The list of questions were refined and reviewed for clarity. Any unclear or repetitive questions were reviewed and removed or reworded as necessary prior to progressing to the pilot study. Some words in the survey were specific to national defense; therefore, I wrote definitions that would clarify how the terminology would apply to both the polygraph-treatment and no polygraph-treatment groups. In an effort to prevent confusion on word use, review of the definitions was mandatory prior to proceeding to the survey on Survey Monkey. For example, words

such as security and espionage were included in the definitions to ensure proper understanding (see Appendix B).

Variables

The operational variable was deterrence effect by means of self-reported perceptions of sanction risk to prior unlawful behavior or continuing acceptable behavior. The variable had two factors from which the questions on the questionnaire were derived: (a) admittance in a change of behavior and attitude and (b) belief of the effects of a change in the workplace security because of the use of the polygraph to ensure compliance. The creation of the questionnaire relied on the development of both factors once the factor analysis was completed.

The overall deterrence effect was determined by *t* test evaluations of the factors that resulted from the exploratory factor analysis, the results of the combination of various survey questions that best answered the research questions, and comparison of both groups with all questions evaluated using a *t* test with alpha set at .05. The scores were calculated by adding the sums of the answers from the Likert scale. Higher scores indicated an increased support for uses of the polygraph examination and self-reported change in behavior and attitude, which enhanced support of polygraph use.

Data Analysis Plan

In this section I discussed the data analysis, which includes descriptive statistics and factor analysis. I also provided in-depth discussions of how each research question and hypotheses were analyzed. This section is organized in the following subsections: data analysis and research questions and hypotheses.

Data Analysis

In this section, I discussed the descriptive statistics used in the study. In addition, I discussed the factor analysis that was performed. This subsection is organized in the following areas: descriptive statistics and factor analysis.

Descriptive statistics. Data were analyzed using SPSS. Descriptive statistics were obtained to describe the research variables used in the analysis. These included means, standard deviations, and *t* tests.

Factor analysis. A factor analysis was conducted among the 30 polygraph questions. A principal component analysis (PCA) was used. The PCA can be used to discover subsets of questionnaire questions that correlate with one another but are independent of another subset of correlated questions (Tabachnick & Fidell, 2012). It was assumed that three factors would be produced: (a) adherence to security regulations, (b) admittance to change of behavior and attitude if a polygraph test is randomly required, and (c) belief that a polygraph is an effective deterrent against security compromises. The factors were assumed to have no correlation with each other; thus, an orthogonal rotation was used in the loading matrix (Tabachnick & Fidell, 2012). Items were considered strong loaders at .50 or better (Costello & Osborne, 2005)).

The number of factors extracted from the PCA were determined by examining eigenvalues and the scree test. The number of factors used were those that have eigenvalues greater than 1.00 (Tabachnick & Fidell, 2012). In addition, the scree plot obtained was assessed for the slope of the decreasing eigenvalues. In addition, the Kaiser rule of eigenvalues greater than .70 for the communalities was assessed (Mertler &

Vannatta, 2010).

To conduct the principal components analysis, the assumptions of sample size, normality, and absence of outliers were assessed. In order to run the factor analysis, a large sample size should be used. MacCallum, Widaman, Zhang, and Hong (1999) suggested at least 100 participants. This number can increase up to 500 if a very large number of items are used. With a total of 30 questions used in this study's factor analysis, the general rule of thumb of 300 participants was a large enough sample to run the analysis (Comrey & Lee, 1992; Tabachnick & Fidell, 2012). Univariate normality among the items is also important for the analysis to run properly. Univariate normality was assessed using skew. A *z* score derived from skew and its standard error were used to assess for normality. For all *z* scores greater than ±1.96, the variable was significantly skewed and considered for removal from the PCA (Tabachnick & Fidell, 2012). Outliers were assessed for, defined as values greater than 3.29 standard deviations from the mean.

Once the PCA was conducted and factors were determined, a Cronbach's alpha reliability testing was conducted on the factors. George and Mallery's (2010) guidelines for reliability were used, where reliability greater than .90 is excellent, than .80 is good, than .70 is acceptable, than .60 is questionable, and less than .60 is unacceptable. Once good reliability was found for all factors, the summation of the factors was done to create the factor scores.

Research Questions and Hypotheses

In this subsection, I provided in-depth discussions of how each research question and hypotheses were analyzed. This subsection is organized in the following areas:

Research Question 1, Research Question 2, and Research Question 3.

Research Question 1. To what extent are there differences in the likelihood to adhere more closely to security regulations if a polygraph is required as a condition of employment by group (no polygraph-treatment vs. polygraph-treatment)?

$H_0$1: There will be no difference in the likelihood to adhere more closely to security regulations if a polygraph is required as a condition of employment by group (no polygraph-treatment vs. polygraph-treatment).

H_a1: There will be differences in the likelihood to adhere more closely to security regulations if a polygraph is required as a condition of employment by group (no polygraph-treatment vs. polygraph-treatment).

To examine Research Question 1, I conducted an independent sample *t* tests to assess if there were differences in the likelihood to adhere more closely to security regulations if a polygraph is required as a condition of employment by group (no polygraph-treatment vs. polygraph-treatment). The independent sample *t* test was the appropriate analysis to conduct with the goal being to assess statistical differences in a continuous dependent variable by a dichotomous independent variable (Pallant, 2010). In this case, the factor were based on the likelihood to adhere more closely to security regulations if a polygraph is required as a condition of employment was the continuous dependent variable of the test. The dichotomous independent variable was group, with levels: no polygraph-treatment and polygraph-treatment. A *t* test was conducted for each adherence to security regulations factor found from the PCA. An alpha level of .05 was used for the *t* test.

The assumptions of the independent sample *t* test were assessed prior to analysis. Normality was assessed by examining skewness. A *z* score derived from skew and its standard error were used to assess for normality. For *z* scores greater than ±1.96, the variable was considered significantly skewed and normality was not met (Tabachnick & Fidell, 2012). Although normality is an assumption, violations in normality does not have a large effect in *type I error* (Pallant, 2010). Equality of variance was assessed for through the use of Levene's tests. When equality of variance was not met, the Welch estimate for the *t* test was run instead, which does not assume equal variances.

Research Question 2. To what extent are there differences in the changing of behavior and attitude if a polygraph can be randomly administered at work by group (no polygraph-treatment vs. polygraph-treatment)?

$H_0$2: There will be no differences in the changing of behavior and attitude if a polygraph can be randomly administered at work by group (no polygraph-treatment vs. polygraph-treatment).

H_a2: There will be differences in the changing of behavior and attitude if a polygraph can be randomly administered at work by group (no polygraph-treatment vs. polygraph-treatment).

To examine Research Question 2, I conducted an independent sample *t* test to assess if there were differences in the changing of behavior and attitude if a polygraph can be randomly administered at work by group (no polygraph-treatment vs. polygraph-treatment). The independent sample *t* test is the appropriate analysis to conduct when the goal is to assess for statistical differences in a continuous dependent variable by a

dichotomous independent variable (Pallant, 2010). In this case, the factors that were based on changing the behavior and attitude if a polygraph can be randomly administered at work were the continuous dependent variable of the test. The dichotomous independent variable was group, with levels: no polygraph-treatment and treatment. A *t* test was conducted for each adherence to security regulations factor found from the PCA. An alpha level of .05 was used for the *t* test.

The assumptions of the independent sample *t* test were assessed prior to analysis. Normality was assessed by examining skewness. A *z* score derived from skew and its standard error were used to assess for normality. For the z scores greater than ±1.96, then the variable was considered significantly skewed and normality was not met (Tabachnick & Fidell, 2012). Although normality is an assumption, violations in normality does not have a large effect in *type I error* (Pallant, 2010). Equality of variance was assessed for by the use of Levene's tests. When equality of variance was not met, the Welch estimate for the *t* test was run instead, which does not assume equal variances.

Research Question 3. To what extent are there differences in the belief that a polygraph is an effective deterrent against security compromises by group (no polygraph-treatment vs. polygraph-treatment)?

$H_0$3: There will be no differences in the belief that a polygraph is an effective deterrent against security compromises by group (no polygraph-treatment vs. polygraph-treatment).

H_a3: There will be differences in the belief that a polygraph is an effective deterrent against security compromises by group (no polygraph-treatment vs. polygraph-treatment).

To examine Research Question 3, I conducted an independent sample *t* test to assess if there were differences in the belief that a polygraph is an effective deterrent against security compromises by group (no polygraph-treatment vs. polygraph-treatment). The independent sample *t* test is the appropriate analysis to conduct when the goal is to assess for statistical differences in a continuous dependent variable by a dichotomous independent variable (Pallant, 2010). In this case, the factors that were based on the belief that a polygraph is an effective deterrent against security compromises were continuous dependent variable of the test. The dichotomous independent variable was group, with levels: no polygraph-treatment and treatment. A *t* test was conducted for each adherence to security regulations factor found from the PCA. An alpha level of .05 was used for the *t* test.

The assumptions of the independent sample *t* test were assessed prior to analysis. Normality was assessed by examining skewness. A *z* score derived from skew and its standard error were used to assess for normality. For *z* scores greater than ±1.96, the variable was considered significantly skewed and normality was not met (Tabachnick & Fidell, 2012). Although normality is an assumption, violations in normality does not have a large effect in *type I error* (Pallant, 2010). Equality of variance was assessed for by way of Levene's tests. When equality of variance was not met, the Welch estimate for the *t* test was run instead, which does not assume equal variances.

Threats to Validity

In this section, I discussed threats to the validity of the survey. In addition, I discussed informed consent and ethical considerations. This section is organized in the following subsections: threats to validity of the instrument and ethical procedures.

Threats to Validity of the Instrument

The survey design has many strengths, but it also has several weaknesses. In relation to this study, one of the possible validity threats of the survey design is that surveys are inflexible in many ways (Babbie, 2007). A 5-point Likert scale format was used and participants may be resistant to this format. Even though definitions were provided to help ensure full understanding of the questions asked, when filling out the surveys, participants may find some questions ambiguous. Since the survey was conducted through Survey Monkey, I was not present to provide additional information to participants. However, participants were provided with my contact information on the consent form in case they had any questions.

Selection or sampling bias was an external threat to validity. In regard to selection bias, since I am a polygraph examiner and some of the participants received their screening examination from me, participants may expect preferential treatment. However, participants were informed on the consent form that there were no connections between the study and their examination; therefore, they should not expect any preferential treatment as a result of their voluntary participation in the study. Nonresponse bias is also another threat, which could have resulted in a low response rate on the survey and a decrease in the sample size, which could also affect the generalizability of the data. Some

surveys could not be used as some participants did not complete all the questions. However, there was enough participation to meet the sample size needed, where 300 participants was the minimum and 326 individuals participated in the study.

An internal threat to validity was the development of the survey and ensuring its reliability and validity. To address this threat, I used the assistance of experts in the field in developing my survey questions and conducted a pilot study before using the survey in the main study.

Ethical Procedures

The study was conducted in accordance with the parameters established by Walden University's IRB to ensure the ethical protection of research participants. Hard copy consent forms were provided to participants during recruitment and an electronic consent form was also provided on Survey Monkey (see Appendix A). Participation in the study replied on implicit endorsement rather than signed endorsement. Participants were anonymous as no demographic data were collected. I did not knowingly recruit individuals from vulnerable populations. I also did not recruit volunteers under 18 years old and ensured that participants were U.S. citizens or resident aliens. I also excluded individuals who had pending polygraphs with me.

The consent form outlined participants' protections and the ethical guidelines I followed during the research project. The consent form included my contact information in case individuals had questions at any time before, during, or after the study. In addition, the consent form included the selection criteria for the study, outlined risks (physical or psychological) that the participants might experience, and participants were

informed that they were not obligated to complete any parts of the study with which they were not comfortable. In addition, the consent form outlined the anticipated benefits of the study, the lack of compensation, privacy information, disclosure of any potential conflicts of interest, and the contact information of the Walden University representative with whom they could privately talk about their rights as participants. Participants were also informed that all data will be kept on removable media in a safe accessible only to me for a period of 5 years.

Summary

In this study, I determined the perceived deterrent effect related to the use of polygraphs between a group of participants who were subjected to a polygraph examination within the past year compared to those who have not experienced a polygraph examination within the same time period. There were152 participants in the polygraph-treatment group and 174 participants in the no polygraph-treatment group (N = 326). Data were analyzed with a t test to determine whether there was a statistically significant difference between the groups. I also conducted an exploratory factor analysis to determine factors related to deterrence. Data were analyzed using the SPSS.

The instrumentation for this study was a 15-minute researcher-developed questionnaire that was used to obtain the perceptions of participants about the perceived deterrence effect related to the use of polygraphs. A pilot study was conducted on the survey prior to the main study. All individuals were given a hard copy consent form with the survey link on Survey Monkey. The consent form was also available on Survey Monkey and implied consent was used. To ensure anonymity, no demographic

information was collected. All nonattributable digital data from the questionnaires are kept on removable media in a safe accessible only to me for a period of 5 years. Participants were provided with my contact information and the Walden University representative's telephone number.

In Chapter 3, I included the introduction, research design and rationale, methodology, data analysis plan, threats to validity, and a summary of the chapter. In Chapter 4, I include the introduction, pilot study, data collection and study results, and a summary of the chapter. In Chapter 5, I include the introduction, interpretation of findings, limitations of the study, recommendations, implications, and a conclusion to the study.

Chapter 4: Results

Introduction

In this study, I determined the perceived deterrent effect related to the use of polygraphs between a group of participants who were subjected to a polygraph examination within the past year compared to those who have not experienced a polygraph examination within the same time period. Three research questions were examined. The first research question determined the differences between the two groups of adhering more closely to security regulations if a polygraph is required as a condition of employment. The second research question determined the differences between the two groups in the changing of behavior and attitude if a polygraph can be randomly administered at work. The third research question determined the differences between the two groups in their beliefs that a polygraph is an effective deterrent against security compromises. In Chapter 4, I present the pilot study, data collection and study results, and a summary of the chapter.

Pilot Study

A pilot study was conducted in December 2014. The purpose of the pilot study was to determine the reliability of the questions on the survey and the feasibility of implementing the data collection methodology. I collected at least 25 surveys in each of the polygraph-treatment and no polygraph-treatment groups (polygraph-treatment $N = 26$; no polygraph-treatment $N = 56$). Based on Field's (2005) guidelines, 82 was a relatively small number for conducting an exploratory factor analysis. The factor analysis, however, produced a six-factor solution. When examining factor loadings greater than .50, one

factor had only one question to it (Factor 5). I ran Cronbach's alpha reliability testing on each of the factor solutions. Factors 1 – 4 had excellent reliability (>.90). However, factor 6 had poor reliability (.40). Therefore, the pilot study produced four good factors to use. Below are the questions that relate to each factor:

- Factor 1: q15, q18, q27, q28, q32, and q41
- Factor 2: q16, q17, q24, q25, q26, q29, q31, q37, and q42
- Factor 3: q34, q35, q45, and q46
- Factor 4: q19, q20, q21, and q22

Questions that could have been dropped from this list were q13, q14, q30, q33, q36, q39, q40, q43, and q44 because they cross-loaded or were present to detect answering bias and would not have been evaluated. I decided to retain all questions due to the inadequate number of survey questions for an adequate exploratory factor analysis. Only five of the proposed questions on the list could have been dropped because the remainder were present to detect answering bias in the survey and would not have been included in the final factor analysis. The methodology of collecting surveys was found to be sufficient for expanded use. If a volunteer made a mistake when filling out the survey, the Survey Monkey website would record a cookie that stated a survey had been completed. The volunteer could not open the survey again without clearing out the cookies. When soliciting volunteers, I had to provide each volunteer with instructions on how to clear out cookies from a web browser.

Data Collection and Study Results

In this section, I discussed the descriptive statistics used in the study. I also discussed the factor analysis and the results of the study. This section is organized in the following subsections: descriptive statistics, factor analysis, and results.

Descriptive Statistics

Originally, 372 participants started the online survey and 326 individuals completed the survey. Therefore, the sample consisted of 326 participants, all of whom were U.S. citizens or legal resident aliens. There were 152 participants in the polygraph-treatment group and 174 participants in the no polygraph-treatment group. Thus, the completion rate for the surveys once a participant had started was 88%. Participants were located in South Korea and the United States. Frequencies and percentages for nominal variables are presented in Table 1. Demographics were not collected due to a guarantee of anonymity and demographics could have been used to identify likely volunteers.

Table 1

Frequencies and Percentages for Nominal Variables

Variables	*n*	%
Taken Polygraph in the Last Year		
No	174	53
Yes	152	47

Note. Due to rounding error, percentages may not add up to 100.

Factor Analysis

To assist in dimension reduction, I conducted a PCA on the 34 survey items. A PCA creates linear combinations of variables without assuming an underlying structure of

data (Suhr, 2005). PCA is commonly used when sample sizes are large, the variables are highly correlated, and the goal is to reduce the number of variables (Suhr, 2005).

I assumed it would produce three factors (adherence to security regulations, admittance to change of behavior and attitude if a polygraph test is randomly required, and belief that a polygraph is an effective deterrent against security compromises) and that the factors would not be correlated. Therefore, I used an orthogonal rotation in the loading matrix (Tabachnick & Fidell, 2012). However, the results on the initial PCA indicated a total of six components, similar in nature to the pilot survey. Upon further examination, the factor correlation matrix indicated that most factors were correlated at .32 or above. Based on Tabachnick and Fidell's (2012) guidelines, any factors above .32 should use oblique rotation methods. Therefore, the PCA was conducted again, implemented a manual constraint of three factors, and used direct oblimin rotation. The first three components had eigenvalues greater than one and cumulatively explained 59% of the variance. The scree plot in Figure 1 shows that the first principal component accounts for the majority of the variance in the items.

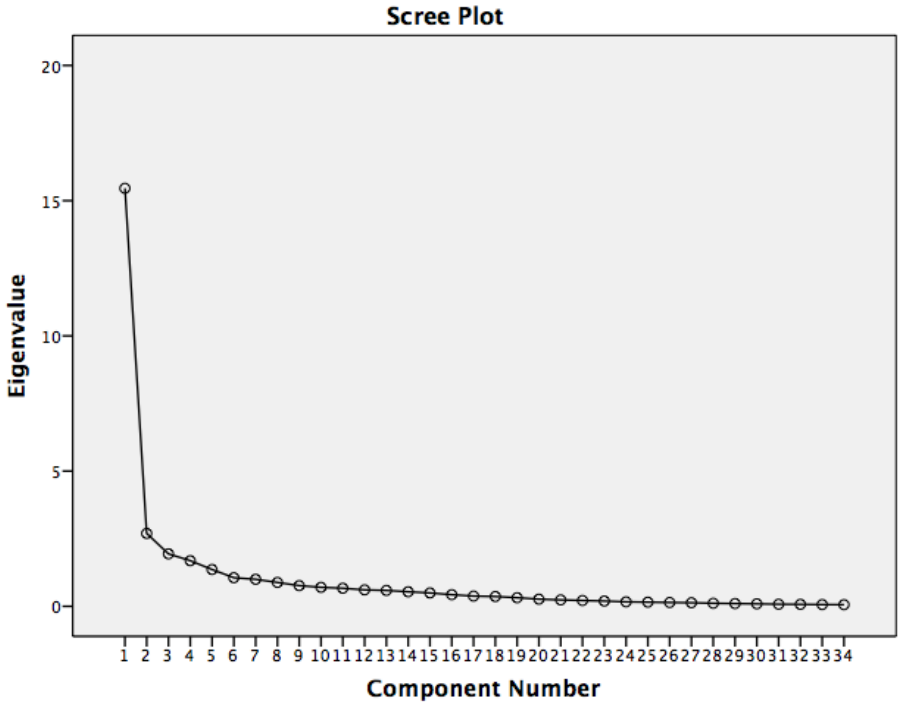

Figure 1. Scree plot for factor loadings.

The first factor consisted of 11 items, the second factor consisted of four items, and the third factor consisted of 12 items. The results of the PCA can be seen in Table 2. The items in each factor produced by the PCA are presented in Table 3.

Table 2

Eigenvalues of the Three Principal Components for Perceptions of Polygraph Examinations

Principal Component	Eigenvalue	% of Variance	Cumulative % of Variance
Comp. 1	15.46	45.46	45.46
Comp. 2	2.70	7.93	53.39
Comp. 3	1.94	5.70	59.09

Table 3

Items in Factors Produced by PCA for Polygraph Examinations Perceptions

Factor 1
RANDOM polygraph exams can help prevent espionage.
RANDOM polygraph examinations can help prevent leaks of classified information.
RANDOM polygraph exams can help prevent deliberate security compromises.
RANDOM polygraph exams can help prevent deliberate security compromises.
RANDOM polygraph exams can enhance workplace security.
A RANDOM polygraph exam can help detect deliberate security compromises.
Those subjected to RANDOM polygraph exams adhere more closely to the security regulations.
As part of a security program, personnel should be subjected to a RANDOM polygraph exam.
People with a high level security clearance should be subjected to a RANDOM polygraph exam.
More frequent polygraph exams can enhance the security of the Department of Defense.
I am willing to take a RANDOM polygraph exam as part of a security program.
Factor 2
I would adhere more closely to security regulations if I were subjected to a MANDATORY polygraph exam.
I adhere more closely to security regulation because I am subjected to a MANDATORY polygraph exam on security regulations.
I adhere more closely to security regulations because I am subjected to a RANDOM polygraph exam on security regulations.
I would adhere more closely to security regulations if I were subjected to a RANDOM polygraph exam.
Factor 3
I am willing to take a MANDATORY polygraph exam in order to enhance a security program.
People with a high level security clearance should be subjected to a MANDATORY polygraph exam.
As part of a security program, personnel should be subjected to a MANDATORY polygraph exam.
A MANDATORY polygraph exam can help detect deliberate security compromises.
MANDATORY polygraph exams can help prevent espionage.
MANDATORY polygraph exams can help prevent deliberate security compromises.

(continued)

MANDATORY polygraph exams can enhance workplace security.
People with a high level security clearance should be given a polygraph exam.
Polygraph exams are a necessary part of a security program.
The results of a polygraph should not be used when making a security decision. (Reverse scored)
I would commit a security violation even if I was subjected to a polygraph exam. (Reverse scored)
Information on RANDOM polygraph examinations should be excluded from MANDATORY Threat Awareness briefings. (Reverse scored)

I examined the factors with regards to the research questions. It indicated that Factor 2 assessed adherence to security regulations and was appropriate to address Research Question 1. This factor contained four items, which were worded in a way that would be suitable for those that have recently taken a screening polygraph within the last year, those that have not taken a screening polygraph within the last year and did not need one for their current job (e.g., "I adhere more closely to security regulations because I am subjected to random polygraphs"), and those who have not taken a polygraph (e.g., "I would adhere more closely to security regulations if I were given a random polygraph"). Therefore, responses that were applicable for participants given categorization were used to create a composite score of two variables (security adherence due to random polygraphs and security adherence due to mandatory polygraphs).

Because the other factors produced by the PCA did not directly assess the remaining research questions, I created new composite scores. A composite score for admittance to change of behavior and attitude if a polygraph test is randomly required (Research Question 2) was created from the mean of seven items and belief that a polygraph is an effective deterrent against security compromises (Research Question 3)

was created from the mean of seven items. These composites, and the items contained in each, are presented in Table 4.

Table 4

Items in Composite Score for Perceptions of Polygraph Examinations

Adherence to Security Regulations
I [would] adhere more closely to security regulations because I am [if I were] subjected to a mandatory polygraph exam.
I [would] adhere more closely to security regulations because I am [if I were] subjected to a random polygraph exam.
Admittance of Behavior and Attitude Change
Those subjected to random polygraph exams adhere more closely to the security regulations.
As part of a security program, personnel should be subjected to a random polygraph exam.
People with a high level security clearance should be subjected to a random polygraph exam.
More frequent polygraph exams can enhance the security of the department of defense.
I am willing to take a random polygraph exam as part of a security program.
People with a high level security clearance should be given a polygraph exam.
Polygraph exams are a necessary part of a security program.
Perceptions of Polygraph Efficacy
Random polygraph exams can help prevent espionage.
Random polygraph exams can help prevent leaks of classified information.
Random polygraph exams can help prevent deliberate security compromises.
Random polygraph exams can enhance workplace security.
Mandatory polygraph exams can help detect deliberate security compromises.
Mandatory polygraph exams can help prevent espionage.
Mandatory polygraph exams can enhance workplace security.

To ensure that each of these composite scores had good internal consistency, I used a Cronbach's alpha analysis for reliability. I used George and Mallery's (2010) guidelines for reliability where reliability greater than .90 is excellent, greater than .80 is

good. I did not use any lower scores for reliability. The composite score for adherence to security regulations had excellent reliability (α = .92). The composite score for admittance to change of behavior and attitude likewise had excellent reliability (α = .90), and the composite score for belief that a polygraph is an effective deterrent had excellent reliability (α = .92). The means, standard deviations, and reliability are presented in Table 5.

Table 5

Means, Standard Deviations, and Reliability for Composite Scores

Variable	*M*	*SD*	α	No. of items
Adherence to Security Regulations	3.29	1.17	.92	2
Admittance of Change of Behavior and attitude	3.90	0.79	.90	7
Effective Deterrent Against Security Compromises	3.76	0.81	.92	7

Results

In this subsection, I discussed the results of the three research questions. The statistical analysis findings are organized by research questions. This subsection is organized in the following areas: Research Question 1, Research Question 2, and Research Question 3.

Research Question 1. To what extent are there differences in the likelihood to adhere more closely to security regulations if a polygraph is required as a condition of employment by group (no polygraph-treatment vs. polygraph-treatment)?

$H_0$1: There will be no difference in the likelihood to adhere more closely to security regulations if a polygraph is required as a condition of employment by group (no polygraph-treatment vs. polygraph-treatment).

H_a1: There will be differences in the likelihood to adhere more closely to security regulations if a polygraph is required as a condition of employment by group (no polygraph-treatment vs. polygraph-treatment).

To examine Research Question 1, I conducted an independent sample *t* test to assess if there were differences in the likelihood to adhere more closely to security regulations if a polygraph is required as a condition of employment by group (taken polygraph in past year: yes vs. no). The independent sample *t* test is the appropriate analysis to conduct when the goal is to assess for statistical differences in a continuous dependent variable by a dichotomous independent variable (Pallant, 2010). The composite score for adherence to security regulations was the continuous dependent variable and group (taken polygraph in past year: yes vs. no) was the independent variable. An alpha level of .05 was used for the test.

Prior to analysis, I assessed the assumption of normality with a Shapiro-Wilk test. The result of the test was significant, $p < .001$, indicating a violation of the assumption of normality. However, Howell (2012) suggests that the *t* test is robust despite violations of normality. The assumption of equality of variance was assessed using Levene's test. The result of the test was not significant, $p = .470$, indicating the assumption of equality of variance was met.

The results of the independent sample *t* test were not significant, $t(324) = 0.55$, $p = .584$, suggesting that there was not a statistically significant difference in adherence to security regulations by group. Therefore, the null hypothesis was accepted and the alternative hypothesis was rejected. Results of the independent sample *t* test are presented in Table 6. Figure 2 shows the average score for adherence to security regulations by group.

Table 6

Independent Sample t Test for Adherence to Security Regulations by Group

				No		Yes
Variable	*t*(324)	*p*	*d*	*M*	*SD*	*M*
Adherence to security regulations	0.55	.584	0.06	3.33	1.18	3.26

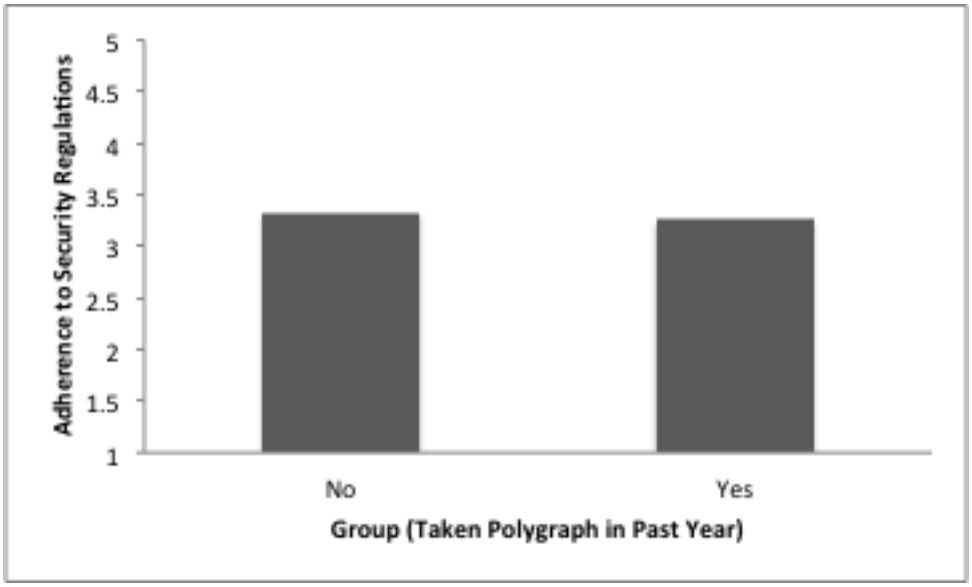

Figure 2. Adherence to security regulations by group (taken polygraph in past year).

Research Question 2. To what extent are there differences in the changing of behavior and attitude if a polygraph can be randomly administered at work by group (no polygraph-treatment vs. polygraph-treatment)?

$H_0$2: There will be no differences in the changing of behavior and attitude if a polygraph can be randomly administered at work by group (no polygraph-treatment vs. polygraph-treatment).

H_a2: There will be differences in the changing of behavior and attitude if a polygraph can be randomly administered at work by group (no polygraph-treatment vs. polygraph-treatment).

To examine Research Question 2, I conducted an independent sample *t* test to assess if there were differences in admittance to change of behavior and attitude if a polygraph test can be randomly administered by group (taken polygraph in the past year: yes vs. no). Prior to the analysis, I assessed the assumption of normality with a Shapiro-Wilk test. The result of the test was significant, $p < .001$, violating the assumption of normality. However, Howell (2012) suggests that the *t* test is robust despite violations of normality. The assumption of equality of variance was assessed using Levene's test. The result of the test was significant, $p = .007$, violating the assumption of equality of variance; therefore, the Welch *t* statistic, which does not assume equality of variance, was used (Stevens, 1999).

The results of the *t* test were significant, $t(321) = -6.09$, $p < .001$, suggesting that there was a difference in admittance to change of behavior and attitude by group. Participants who had not taken a polygraph in the past year scored significantly lower

than participants who had taken a polygraph in the past year. Based on Cohen's (1992) guidelines, the difference between the two groups was a medium effect size. The alternative hypothesis was accepted and the null hypothesis was rejected. Results of the *t* test are presented in Table 7. Figure 3 shows the mean score for admittance to behavior and attitude change by group.

Table 7

Independent Sample t Test for Admittance to Behavior and Attitude Change by Group (Taken Polygraph: Yes vs. No)

				No		Yes
Variable	*t*(321)	*p*	*d*	*M*	*SD*	*M*
Admittance to Behavior and attitude Change	-6.09	.001	0.67	3.66	0.83	4.16

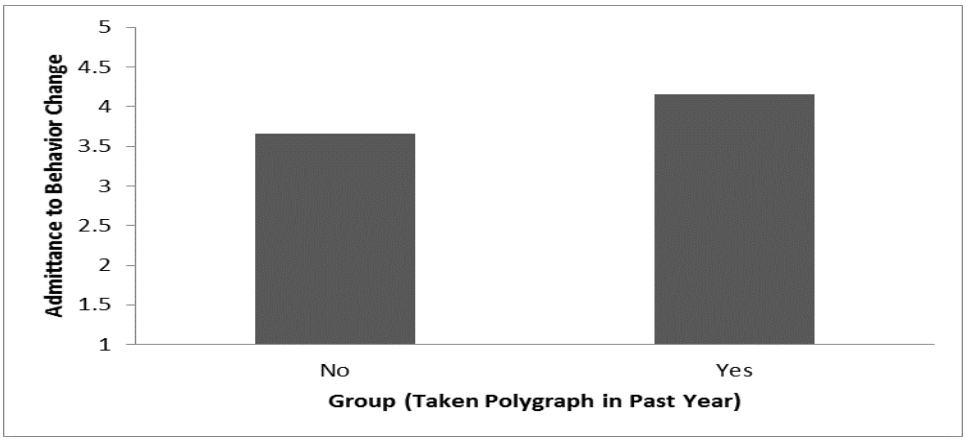

Figure 3. Admittance of behavior and attitude change by group (taken polygraph in the past year.

Research Question 3. To what extent are there differences in the belief that a polygraph is an effective deterrent against security compromises by group (no polygraph-treatment vs. polygraph-treatment)?

$H_0$3: There will be no differences in the belief that a polygraph is an effective deterrent against security compromises by group (no polygraph-treatment vs. polygraph-treatment).

H_a3: There will be differences in the belief that a polygraph is an effective deterrent against security compromises by group (no polygraph-treatment vs. polygraph-treatment).

I conducted an independent samples *t* test to assess if there were differences in perceptions of polygraphs as effective deterrent to security compromises by group (taken polygraph in the past year: yes vs. no). Prior to analysis, I assessed the assumption of normality with a Shapiro-Wilk test. The result of the test was significant, $p < .001$, violating the assumption of normality. However, Howell (2012) suggested that the *t* test is robust despite violations of normality. The assumption of equality of variance was assessed using Levene's test. The result of the test was significant, $p = .008$, violating the assumption of equality of variance; therefore, the Welch *t* statistic, which does not assume equality of variance, was used (Stevens, 1999).

The results of the independent sample *t* test were significant, $t(321) = -7.01$, $p < .001$, suggesting that there was a difference in perceptions of polygraphs efficacy in deterring and preventing security compromises by group. Participants who had not taken a polygraph in the past year scored significantly lower than participants who had taken a

polygraph in the past year. Based on Cohen's (1992) guidelines, the difference between the two groups was a medium effect size. The alternative hypothesis was accepted and the null hypothesis was rejected. Results of the independent sample *t* test are presented in Table 8. Figure 4 shows the mean score for perceptions of polygraphs efficacy in deterring and preventing security compromises by group.

Table 8

Independent Sample t Test for Perceptions of Polygraphs Efficacy in Deterring/Preventing Security Compromises by Group (Taken Polygraph: Yes vs. No)

				No		Yes
Variable	*t*(321)	*p*	*d*	*M*	*SD*	*M*
Perceptions of Polygraphs efficacy in deterring/preventing security compromises	-7.01	.001	0.77	3.49	0.83	4.07

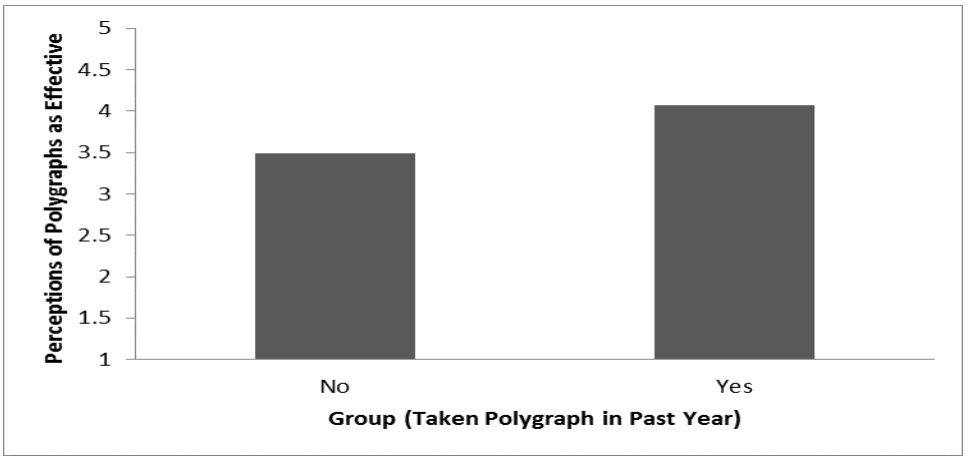

Figure 4. Perceptions of polygraphs efficacy by group (taken polygraph in past year).

Summary

Two of the three research questions had statistically significant results, which indicated a deterrent effect with regards to utility of a polygraph with those who had recently taken a polygraph examination within the last year. Specifically, for Research Question 2, the results indicated that there is a significant difference in the changing of behavior and attitude if a polygraph can be randomly administered at work by group. For Research Question 3, results indicated that there is a significant difference in the belief that a polygraph is an effective deterrent against security compromises by group. On the other hand, for Research Question 1, findings indicated no significant difference in the likelihood to adhere more closely to security regulations if a polygraph is required as a condition of employment by group. However, when reviewing Research Question 1 factors, it is interesting to note that those who have not taken a polygraph within the past year and do not require a polygraph as part of their current job were more likely to display a supportive attitude towards increased adherence to security regulations. In Chapter 4, I included the introduction, pilot study, data collection and study results, and a summary of the chapter. In Chapter 5, I include the introduction, interpretation of findings, limitations of the study, recommendations, implications, and a conclusion to the study.

Chapter 5: Discussion, Conclusions, and Recommendations

Introduction

In this descriptive and exploratory research study, I determined whether there was a perceived deterrent effect related to the use of polygraphs between a group of participants who were subjected to a polygraph examination within the past year compared to those who have not experienced a polygraph examination within the same time period. The instrumentation for this study was a 15-minute researcher-developed questionnaire that was used to obtain the perceptions of participants about the perceived deterrence effect related to the use of polygraphs. This study was designed to answer three research questions: (a) To what extent are there differences in the likelihood to adhere more closely to security regulations if a polygraph is required as a condition of employment by group (no polygraph-treatment vs. polygraph-treatment), (b) to what extent are there differences in the changing of behavior and attitude if a polygraph can be randomly administered at work by group (no polygraph-treatment vs. polygraph-treatment), and (c) to what extent are there differences in the belief that a polygraph is an effective deterrent against security compromises by group (no polygraph-treatment vs. polygraph-treatment)?

The results of the study indicated that there is a significant difference in the changing of behavior and attitude if a polygraph can be randomly administered at work by group. In addition, findings indicated a significant difference in the belief that a polygraph is an effective deterrent against security compromises by group. On the other hand, findings indicated no significant difference in the likelihood to adhere more closely

to security regulations if a polygraph is required as a condition of employment by group. In Chapter 5, I discussed the interpretation of findings, limitations of the study, recommendations, implications, and a conclusion to the study.

Interpretation of the Findings

In an effort to determine whether there was a perceived deterrence effect related to the use of polygraphs, this descriptive and exploratory research study examined three research questions. The finding are interpreted in the context of the theoretical foundation and the literature review. This section is organized in the following subsections: Research Question 1, Research Question 2, and Research Question 3.

Research Question 1

To what extent are there differences in the likelihood to adhere more closely to security regulations if a polygraph is required as a condition of employment by group (no polygraph-treatment vs. polygraph-treatment)? The results of the independent sample *t* test were not significant, $t(324) = 0.55$, $p = .584$, suggesting that there was not a statistically significant difference in adherence to security regulations by group. Therefore, the null hypothesis was accepted and the alternative hypothesis was rejected.

The research results revealed that individuals already subjected to a polygraph were not more likely to adhere more closely to security regulations as a result of being subjected to a polygraph examination. This finding may be attributed to the complacency within the Executive Branch in prosecuting security compromises (Pozen, 2013). Pozen (2013) noted that security compromises of classified information are very difficult to prosecute. Even though there have been over 100 successful prosecutions for espionage,

there are probably hundreds of security compromises of classified information every year to the media (PERSEREC, 2009; Pozen, 2013). Pozen highlighted that there are few successful prosecutions despite the huge number of leaks. This also relates to Bandura's (1974, 1977, 1986) SLT as it takes into account individuals' past experiences, which influences reinforcement, expectations, and expectancies (Boston University School of Public Health, 2013). All of these factors shape whether individuals will engage in a specific behavior and their reasons for doing so (Boston University School of Public Health, 2013).

In addition, the lack of difference in adherence to security regulations between the two groups can also be interpreted in the context of Vance and Siponen's (2012) rational choice model as organizational context factors could indirectly influence individual employees' compliance intention, which is influenced by perceived benefits, formal sanctions, and security risks (Li et al., 2010). The effect of sanction severity was found to be moderated by personal norms (CITE). Similarly, in relation to Paternoster and Simpson's (1996) rational choice model, Paternoster and Simpson noted that the decisions of employees are influenced by (a) the risks and benefits they perceive for themselves, (b) the risks and benefits they perceive for their company, and (c) the presence or absence of offending inducements or restrictions within the specific context of the organization.

Research Question 2

To what extent are there differences in the changing of behavior and attitude if a polygraph can be randomly administered at work by group (no polygraph-treatment vs.

polygraph-treatment)? The results of the *t* test were significant, $t(321) = -6.09$, $p < .001$, suggesting that there was a difference in admittance to change of behavior and attitude by group. Based on Cohen's (1992) guidelines, the difference between the two groups was a medium effect size. The alternative hypothesis was accepted and the null hypothesis was rejected.

The research results revealed that participants who had not taken a polygraph in the past year or ever scored significantly lower than participants who had taken a polygraph in the past year. Therefore, individuals who are subjected to random polygraph testing are more likely aware of certain consequences to polygraph testing, such as detection and subsequent punishment (Nagin & Paternoster, 1991; Nagin & Pogarsky, 2003; Paternoster et al., 1983a; Watson, 1986; Wright, 2010). The National Research Council (2003) noted that individuals who are subjected to polygraph testing will either resign to avoid the exam and subsequent interrogation, decide not to engage in a prohibited behavior, or simply avoid a particular agency altogether. For those subjected to polygraph testing on a regular basis in order to gain continued access to sensitive programs, the desired effect is that of continued adherence to rules, self-directed behavior and attitude change, or modification (Nagin & Paternoster, 1994; Nagin & Pepper, 2012; ODNI, 2015a; U.S. Army, 1993).

The significant differences in the changing of behavior and attitude if a polygraph can be randomly administered at work by group can also be interpreted in the context of Paternoster and Simpson's (1996) rational choice model as employees who are subjected to random polygraph testing at the individual level may be more aware of the potential

costs of wrongdoing, such as the severity of formal sanctions, and other potential costs such as loss of occupational position; social censure from colleagues, family, and friends; personal embarrassment, and shame. In addition, the employees in the polygraph-treatment group may be more dissuaded from offending if the organization or a staff member has recently been sanctioned for similar conduct or the company has organizational restraints such as an ethics hotline or random polygraph testing (Paternoster & Simpson, 1996). Furthermore, employees in the polygraph-treatment group may be more affected by normative factors such as their moral evaluation of wrongdoing (Paternoster & Simpson, 1996). According to Paternoster and Simpson, employees may be restrained by moral inhibitions; therefore, some acts of corporate crime are not committed because they are believed to be wrong.

Similarly, the findings can also be interpreted in the context of Vance and Siponen's (2012) rational choice model as the polygraph-treatment group may have higher considerations for the severity of possible formal and informal sanctions, their moral beliefs, and perceived benefits, such as incentives, when considering policy or organizational violations. For example, D'Arcy et al. (2009) found that only the severity of formal sanctions effectively reduced IS misuse. Bandura's (1974, 1977, 1986) SLT can also be applied to the findings as employees in the polygraph-treatment group likely anticipated the consequences of their behaviors at a higher level than the no polygraph-treatment group. Therefore, the polygraph-treatment group anticipated the consequences of their actions before they engaged in the behavior and these anticipated consequences influenced the successful completion of the behavior. In addition, the employees in the

polygraph-treatment group appeared to learn by observing what others do, consider the consequences that others experienced, rehearse (mentally first) what might happen in their own lives if they followed other's behavior, take action by trying the behavior, compare their experiences with what happened to others, and confirm their belief in the new behavior.

Research Question 3

To what extent are there differences in the belief that a polygraph is an effective deterrent against security compromises by group (no polygraph-treatment vs. polygraph-treatment)? The results of the independent sample *t* test were significant, $t(321) = -7.01$, $p < .001$, suggesting that there was a difference in perceptions of polygraphs efficacy in deterring and preventing security compromises by group. Based on Cohen's (1992) guidelines, the difference between the two groups was a medium effect size. The alternative hypothesis was accepted and the null hypothesis was rejected.

The research results revealed that participants who had not taken a polygraph in the past year scored significantly lower than participants who had taken a polygraph in the past year. This finding may be attributed to employees in the polygraph-treatment group beliefs about its use, its effectiveness, and the certainty of crime detection. Research on criminal deterrence indicated that certainty of detection has a much greater deterrent effect on employees (Nagin & Paternoster, 1991, 1994; Nagin & Pogarsky, 2001; Paternoster et al., 1983a). Therefore, employees in the polygraph-treatment group appear to be more aware that there are certain consequences to wrongdoing (Nagin & Paternoster, 1991; Nagin & Pogarsky, 2003; Paternoster et al., 1983a; Watson, 1986),

which could be detected by means of polygraph analysis. Wright (2010) noted that employees who leak information should be aware that there is an increased likelihood of detection and subsequent punishment. Therefore, employees who are subjected to polygraph testing will either resign to avoid the exam and subsequent interrogation, decide not to engage in a prohibited behavior, or simply avoid a particular agency altogether (National Research Council, 2003). Based on the findings, polygraph testing appears to have a deterrent effect on employees in the polygraph-treatment group who have access to sensitive programs. The desired effect of polygraph analysis is continued adherence to rules, self-directed behavior and attitude change, or modification (Nagin & Paternoster, 1994; Nagin & Pepper, 2012; ODNI, 2015a; U.S. Army, 1993).

The findings can also be interpreted in the context of Paternoster and Simpson's (1996) rational choice model, where the use of polygraph analysis is used to detect and deter wrongdoing. Paternoster and Simpson (1996) found that threats of criminal and civil sanctions directed against the individual inhibited the intention to commit corporate crime as well as the fear of informal sanctions. The threat of legal sanctions may be necessary to maintain the legitimacy of an extensive network of informal and normative controls. Similarly, Li et al. (2010) found that compliance intention will increase when employees perceive high threats from formal or informal sanctions. However, the researchers contended that theoretical models of corporate crime and public policy efforts must contain instrumental (threats of punishment) and deontological (appeals to morality) factors.

The findings of my study can also be interpreted in the context of Bandura's (1974, 1977, 1986) SLT, where employees vicariously learn about punishments from their peers by picking up modeling cues, environmental cues, and social cues in the inhibitive learning process and becoming deterred from committing future fraudulent acts (Yiu et al., 2014). Subsequently, employees are at least minimally rational agents and their conduct is partly guided by the expected consequences of their behavior (Paternoster & Simpson, 1996).

Limitations of the Study

This study had several limitations. First, this study determined the perceived deterrent effect related to the use of polygraphs between two groups; therefore, the study remained distinct in its focus and limited in its scope. This study was not designed to answer questions related to the validity, reliability, or accuracy rates of polygraph examinations. Although these topics may be important to public policy and administration field, psychology field, and the intelligence community, they were not the focus of this research effort.

A second possible limitation of the study included generalizing the results since a cluster sampling of 326 participants, all of whom were U.S. citizens or legal resident aliens located in South Korea and the United States, was used and the results of the study are limited to similar populations of employees. The 152 participants in the polygraph-treatment group had taken the polygraph through the U.S. Army Intelligence Polygraph Program, which has offices in South Korea and Fort Meade, Maryland. The 174 participants in the no polygraph-treatment group were nonintelligence U.S. citizens and

legal resident aliens who lived and worked in South Korea, were students from the Walden University participant pool, and individuals from the Walden University online community site, LinkedIn. These employees' unique perceptions may not be generalizable to other populations.

Third, I used a 15-minute researcher-developed survey, which has not been used in past studies. However, a pilot study was conducted on the survey prior to using it in the main study. In developing the questions used in the survey, I received assistance from two agencies, the NCCA and the U.S. Army Intelligence Polygraph Program. To help establish the validity of the survey, a member of the research department of the NCCA and a retired polygraph examiner and former employee of the CIA also reviewed the survey questions and provided additional comments to the proposed questions to ensure consistency with community standards. In addition, the survey was found to have very high reliability (Cronbach's alpha = >.90).

Fourth, selection or sampling bias was another limitation of the study. In regard to selection bias, since I am a polygraph examiner and some of the participants received their screening examination from me, participants may expect preferential treatment. However, participants were informed on the consent form that there were no connections between the study and their examination; therefore, they should not expect any preferential treatment as a result of their voluntary participation in the study. Future research could exclude participants who have taken a polygraph the researcher. In addition, changes to the populations could be made in future research, where more similar populations are compared. Specifically, two similar groups of participants who

work only in the intelligence community, one group who require polygraph testing within the last year compared to those who either had never experienced a polygraph or the experience was more than a year prior, could be compared and the results compared to the findings found in this study.

A fifth limitation was nonresponse bias. Nonresponse bias could have resulted in a low response rate on the survey and a decrease in the sample size, which could also affect the generalizability of the data. Some surveys could not be used as some participants did not complete all the questions. However, there was enough participation to meet the sample size needed, where 300 participants was the minimum and 326 individuals participated in the study.

A sixth limitation was self-report or social desirability bias. Self-report or social desirability bias has to be considered as participants may want to be perceived positively so they may not respond honestly. In addition, there are problems inherent with self-report data as participants may not accurately or fully self-evaluate themselves. In order to address this bias, the Likert scale format was used, which did not allow participants the freedom to include additional information that they may have felt was important. It was assumed that participants answered honestly to the questions asked on the survey.

Recommendations

Research Question 1 results revealed that individuals already subjected to a polygraph were not more likely to adhere more closely to security regulations as a result of being subjected to a polygraph examination. Therefore, the null hypothesis was accepted and the alternative hypothesis rejected. Based on this finding, future research

could incorporate the perceptions of participants about the use of polygraph testing with other screening or investigative information that they have undergone to determine if a multifaceted approach would result in a significant difference between the groups in relation to the likelihood of adhering more closely to security regulations. For example, the American Polygraph Association (2005) discussed the use of polygraph results in conjunction with other screening or investigative information when making decisions. Jenkins (2013) suggested the use of mouse movement features that are diagnostic of deception for screening surveys. Paternoster and Simpson (1996) argued for a multifaceted approach to corporate crime control, such as the use of moral education (e.g., business ethics) and legal sanctions. Vance and Siponen (2012) suggested that organizations should include other means to discourage security violations apart from formal sanctions because they are not always effective in deterring policy violations.

As discussed in the limitations of the study, to reduce sampling or selection bias, it is recommended that future studies exclude participants who have taken a polygraph from the researcher as participants may expect preferential treatment. In addition, another previously discussed recommendation was the use of similar populations between the groups that are being compared. Therefore, using two similar groups of participants who work only in the intelligence community, one group who require polygraph testing within the last year compared to those who either had never experienced a polygraph or the experience was more than a year prior. These results could then be compared to the results found in this study.

In this study, demographic questions were excluded from the survey in order to

protect participants' identities and ensure anonymity. However, while still ensuring anonymity, in future studies, researchers could collect limited demographic information that would not reveal participants' identities, such as gender, race and age group. Then using these demographic data, additional analysis could be conducted to see if there are differences in the responses based on gender, race, and age.

In future studies, researchers could further assess the validity and reliability of the survey instrument with similar populations as well as in other settings and culture. Similarly, researchers could also replicate the study using the same methods, but with a similar population, and in different settings and culture as well. The results of these studies could ensure that the results found in this study are valid and reliable, determine the role of extraneous variables, and inspire new research based on findings.

Future research could also focus on modifying the survey's 5-point Likert scale format to a 4-point Likert scale format by removing the neutral option. Researchers have suggested that when presented with a neutral response option, participants will be more likely to select that option than report their actual opinion (Bishop, 1987; Edwards & Smith, 2014; Johns, 2005; Kalton, Roberts, & Holt, 1980; Krosnick et al., 2001; Nowlis, Kahn, & Dhar, 2002).

Implications

Even though the findings for Research Question 1 indicated no significant difference in the likelihood to adhere more closely to security regulations if a polygraph is required as a condition of employment by group, the findings for Research Questions 2 and 3 were statistically significant. The findings indicated that there is a significant

difference in the changing of behavior and attitude if a polygraph can be randomly administered at work by group and there is a significant difference in the belief that a polygraph is an effective deterrent against security compromises by group.

Based on these findings, there was a perceived deterrence effect related to the use of polygraphs between the two groups. At the individual level, employees in sensitive positions who face random polygraph testing may take greater care to avoid even minor security infractions in order to avoid the possibility of a future deceptive reading on a polygraph test. At the policy and organizational levels, one of the goals of polygraph testing is deterrence, which means keeping employees, who have committed or may engage in wrongdoing, out of sensitive positions and keeping employees who are already in sensitive positions from doing undesired activities (National Research Council, 2003). The findings of Research Question 2 that random polygraph testing may result in a change of behavior and attitude is significant as it may deter actions that threaten national interests based on the perceived likelihood and consequences of detection. Therefore, the implications for positive social change stemming from these findings include recommendations to the nation's national security agencies to continue enforcing the polygraph examinations required of certain security personnel and exploring the possibility of expanding the use of such strategies in order to fortify the national intelligence infrastructure.

The findings for Research Question 1 indicated no significant difference in the likelihood to adhere more closely to security regulations if a polygraph is required as a condition of employment by group. Therefore, as noted in the recommendations section,

organizations should use multifaceted approach, where polygraph testing is used in conjunction with other screening or investigative information when making decisions. A multifaceted approach could include the use of polygraph testing, along with mouse movement features that are diagnostic of deception for screening surveys, moral education, and legal sanctions (American Polygraph Association, 2005; Jenkins, 2013; Paternoster & Simpson, 1996; Vance & Siponen, 2012).

While there is an abundance of literature on the reliability and validity of polygraph analysis, this research study added to the literature by filling a gap in the public policy and administration literature with respect to employees' perceptions about the deterrence effect of polygraph analysis. Findings from this study are beneficial not only to the public policy and administration field, but to a wide array of other fields, including the fields of psychology and intelligence. The findings from the study are also applicable to many agencies and organizations, to include the DOD and the coalition of 17 agencies and organizations that are a part of the U.S. Intelligence Community including the ODNI, Army Intelligence, FBI, and CIA.

Conclusion

This study was undertaken in order to determine whether there was a perceived deterrent effect related to the use of polygraphs between a group of participants who were subjected to a polygraph examination within the past year compared to those who have not experienced a polygraph examination within the same time period. Findings indicated a significant difference in the changing of behavior and attitude if a polygraph can be randomly administered at work by group. In addition, findings indicated a significant

difference in the belief that a polygraph is an effective deterrent against security compromises by group. In contrast, findings indicated no significant difference in the likelihood to adhere more closely to security regulations if a polygraph is required as a condition of employment by group.

Malicious insider threats pose a serious threat to organizations (Jenkins, 2013). Polygraph analysis is used as a deterrence to keep potential employees out of sensitive positions and keep current employees who are in sensitive positions from engaging in wrongdoing (American Polygraph Association, 2002; Jenkins, 2013; National Research Council, 2003; ODNI, 2012). Based on the findings, national security agencies should continue their enforcement of polygraph examinations that are required of certain security personnel. In addition, they should seek out other ways to expand polygraph analysis in order to strengthen the national intelligence infrastructure. This could include using a multifaceted approach that would include the use of polygraph testing in conjunction with other mitigation strategies and detection techniques, as well as other screening or investigative information (American Polygraph Association, 2005; Jenkins, 2013; Paternoster & Simpson, 1996; Vance & Siponen, 2012).

References

Abrams, S., & Abrams, J. B. (1993). *Polygraph testing of the pedophile*. Portland, OR: Ryan Gwinner Press.

Aftergood, S. (2012). *Document collector charged under espionage statute*. Retrieved from http://blogs.fas.org/secrecy/2012/11/collector_charged/

Akers, R. L. (1977). *Deviant behavior: A social learning approach* (2nd ed.). Belmont, CA: Wadsworth.

Akers, R. L. (1985). *Deviant behavior: A social learning approach* (3rd ed.). Belmont, CA: Wadsworth.

Akers, R. L. (1990). Rational choice, deterrence, and social learning theory in criminology: The path not taken. *Journal of Criminal Law and Criminology*, *81*, 653-676. doi:10.2307/1143850

Alder, K. (1998). To tell the truth: The polygraph exam and the marketing of American expertise. *Historical Reflections / Réflexions Historiques*, *24*(3), 487-525. Retrieved from http://journals.berghahnbooks.com/hrrh/

American Polygraph Association. (2005). *Polygraph: Issues & answers*. Retrieved from http://www.polygraph.org/

American Polygraph Association. (2013). *Frequently asked questions*. Retrieved from http://www.polygraph.org/section/resources/frequently-asked-questions

Apel, R. (2013). Sanctions, perceptions, and crime: Implications for criminal deterrence. *Journal of Quantitative Criminology*, *29*, 67-202. doi:10.1007/s10940-012-9170-1

Associated Press. (2013, January 2). CIA whistleblower John Kiriakou given more than two years in prison. *The Guardian*. Retrieved from http://www.guardian.co.uk/world/2013/jan/25/cia-whistleblower-john-kiriakou-prison

ASTM International. (2005). *Standard terminology relating to forensic psychophysiology*. Retrieved from http://www.astm.org/Standards/E2035.htm

Babbie, E. (2007). *The practice of social research* (11th ed.). Belmont, CA: Thompson Wadsworth.

Bachman, R., Paternoster, R., & Ward, S. (1992). The rationality of sexual offending: Testing a deterrence/rational choice conception of sexual assault. *Law and Society Review*, *26*, 343-372. doi:10.2307/3053901

Bandura, A. (1974). Behavior theory and the models of man. *American Psychologist*, *29*, 859-869. doi:10.1037/h0037514

Bandura, A. (1977). *Social learning theory*. Englewood Cliffs, NJ: Prentice-Hall.

Bandura, A. (1986) *Social foundations of thought and action: A social cognitive theory*. Englewood Cliffs, NJ: Prentice-Hall.

Becker, G. S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy, 76*, 169-217. doi:10.1086/259394

Bishop, G. F. (1987). Experiments with the middle response alternative in survey questions. *Public Opinion Quarterly*, *51*, 220-232. doi:10.1086/269030

Blau, P. M. (1964). *Exchange and power in social life*. New York, NY: John Wiley.

Borack, J. I. (1998). An estimate of the impact of drug testing on the deterrence of drug use. *Military Psychology, 10,* 17-25. doi:10.1207/s15327876mp1001_2

Boss, S., Kirsch, L., Angermeier, I., Shingler, R., & Boss, R. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems, 18,* 151-164. doi:10.1057/ejis.2009.8

Boston University School of Public Health. (2013). *The social cognitive theory*. Retrieved from http://sphweb.bumc.bu.edu/otlt/MPH-Modules/SB/SB721-Models/SB721-Models5.html

Bunn, G. C. (1997). The lie detector, wonder woman and liberty: The life and work of William Moulton Marston. *History of the Human Sciences, 10,* 91-119. doi:10.1177/095269519701000105

Cochrane, R. E., Tett, R. P., & Vandecreek, L. (2003). Psychological testing and the selection of police officers: A national survey. *Criminal Justice and Behavior, 30,* 511-537. doi:10.1177/0093854803257241

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). New York, NY: Academic Press.

Cohen, J. (1992). A power primer. *Psychological Bulletin, 112,* 155-159. doi:10.1037//0033-2909.112.1.155

Coleman, J. (1973). *The mathematics of collective action*. Chicago, IL: Aldine.

Computer Emergency Readiness Team. (2015). *Insider threat*. Retrieved from http://www.cert.org/insider_threat/

Comrey, A., & Lee, H. (1992). *A first course in factor analysis*. Hillsdale, NJ: Erlbaum.

Cook, K. S. (1977). Exchange and power in networks of interorganizational relations. *Sociological Quarterly, 18*, 62-82. doi:10.1111/j.1533-8525.1977.tb02162.x

Costello, A., & Osborne, J. (2005). Best practices in exploratory factor analysis: Four recommendations for getting the most from your analysis. *Practical Assessment, Research and Evaluation, 10*(7), 1-9. Retrieved from http://pareonline.net/

Cumming, A. (2009). *Polygraph use by the department of energy: Issues for Congress* (CRS Report No. 7-5700). Retrieved from https://www.fas.org/sgp/crs/intel/RL31988.pdf

D'Arcy, J., Hovav, A., & Galletta, D. F. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*, 79-98. doi:10.1287/isre.1070.0160

Dietrich, F., & List, C. (2013). A reason-based theory of rational choice. *Noûs, 47*, 104-134. doi:10.1111/j.1468-0068.2011.00840.x

Ducan, L., Lafree, G., & Piquero, A. R. (2005). Testing a rational choice model of airline hijackings. *Criminology, 43*, 1031-1065. doi:10.1111/j.1745- 9125.2005.00032.x

Edwards, M. L., & Smith, B. C. (2014). The effects of the neutral response option on the extremeness of participant responses. *Psychology, Research, 6*. Retrieved from http://blogs.longwood.edu/incite/2014/05/07/the-effects-of-the-neutral-response-option-on-the-extremeness-of-participant-responses/

Elis, L. A., & Simpson, S. (1995). Informal sanction threats and corporate crime: Additive versus multiplicative models. *Journal of Research in Crime and Delinquency*, *32*, 399-424. doi:10.1177/0022427895032004002

Elsea, J. (2013). *The protection of classified information: The legal framework* (CRS Report No. 7-5700). Retrieved from http://fas.org:8080/sgp/crs/secrecy/RS21900.pdf

Executive Branch. (2008). *Executive Order 12333 - United States intelligence activities*. Retrieved from http://www.archives.gov/federal-register/codification/executive-order/12333.html

Field, A. (2009). *Discovering statistics using SPSS* (3rd ed.). London, England: Sage.

Figliuzzi, C. F. (2012). *Statement before the House Committee on homeland security, subcommittee on counterterrorism and intelligence*. Retrieved from https://www.fbi.gov/news/testimony/economic-espionage-a-foreign-intelligence-threat-to-americans-jobs-and-homeland-security

Foster, M. (2006). *Help your employees avoid the dangers of Internet misuse*. Retrieved from https://www.fosterinstitute.com/articles/intmisuse/pdf/im09_help%20your%20employees%20to%20avoid%20the%20dangers%20of%20internet%20misuse.pdf

George, D., & Mallery, P. (2010). *SPSS for windows step by step: A sample guide and reference* (11th ed.). Boston, MA: Allyn and Bacon.

Gougler, M., Nelson, R., Handler, M., Krapohl, D., Shaw, P., & Bierman, L. (2011). Meta-analytic survey of criterion accuracy of validated polygraph techniques. *Polygraph*, *40*(4), 197-202. Retrieved from https://apoa.memberclicks.net/meta-analytic-survey-of-criterion-accuracy-of-validated-polygraph-techniques

Grasmick, H. G., & Bursik, R. (1990). Conscience, significant others, and rational choice: Extending the deterrence model. *Law and Society Review, 24,* 837-862. doi:10.2307/3053861

Handler, M., & Nelson, R. (2015, March 23). *Principles of applied psycho-physiology and polygraph testing*. Retrieved from https://apoa.memberclicks.net/assets/docs/TDLR/3.23.15-principles-of-applied-psychophysiology-and-polygraph-testing.pdf

Health Communication Capacity Collaborative. (2015). *Social learning theory.* Retrieved from http://www.healthcommcapacity.org/wp-content/uploads/2014/09/SocialLearningTheory.pdf

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18,* 106-125. doi:10.1057/ejis.2009.6

Holmlund, L., Mucisko, D., Kimberland, K., & Freyre, J. (2010). *2010 cybersecurity watch survey: Cybercrime increasing faster than some company defenses*. Retrieved from http://resources.sei.cmu.edu/asset_files/News/2010_100_001_53454.pdf

Holmlund, L., Mucisko, D., Lynch, R., & Freyre, J. (2011). *2011 cybersecurity watch survey: Organizations need more skilled cyber professionals to stay secure*. Retrieved from http://www.cert.org/archive/pdf/CyberSecuritySurvey2011.pdf

Homans, G. (1961). *Social behavior: Its elementary forms*. New York, NY: Harcourt, Brace and World, Inc.

Howell, D. (2012). *Statistical methods for psychology* (8th ed.). Boston, MA: Wadsworth Publishing.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2010). The centrality of low self-control in internal computer offenses. In B. Molyneux (Ed.), *Proceedings of the Dewald Roode information security workshop 2010* (pp. 316-345). Waltham, MA: Bentley University.

Jerkins, J. L. (2013). *Alleviating insider threats mitigation strategies and detection techniques* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 3587255)

Johns, R. (2005). One size doesn't fit all: Selecting response scales for attitude items. *Journal of Elections, Public Opinion and Parties*, *15*, 237-264. doi:10.1080/13689880500178849

Kalton, G. G., Roberts, J., & Holt, D. D. (1980). The effects of offering a middle response option with opinion questions. *The Statistician, 29*, 65-78. doi:10.2307/2987495

Kleinmuntz, B., & Szucko, J. (2004). Lie detection in ancient and modern times: A call for contemporary scientific study. *American Psychologist, 39,* 766-776. doi:10.1037/0003-066x.39.7.766

Koerner, B. I. (2002, December). Lie detector roulette. *Mother Jones*. Retrieved from http://www.motherjones.com/politics/2002/11/lie-detector-roulette

Kohlberg, L. (1976). Moral stages and moralization: The cognitive-developmental approach. In T. Lickona (Ed.), *Moral development and behavior: Theory, research, and social issues* (pp. 31-53). New York, NY: Holt, Rinehart and Winston.

Kohlberg, L. (1984). *The psychology of moral development*. New York, NY: Harper & Row.

Krosnick, J. A., Holbrook, A. L., Berent, M. K., Carson, R. T., Hanemann, W., Kopp, R. J., . . . Conaway, M. (2001). The impact of 'no opinion' response options on data quality: Non-attitude reduction or an invitation to satisfice? *Public Opinion Quarterly, 66,* 371-403. doi:10.1086/341394

Landis, C., & Gullette, R. (1925). Studies of emotional reactions: Systolic blood pressure and inspiration-expiration ratios. *Journal of Comparative Psychology, 5,* 221-253. doi:10.1037/h0074346

Leon, A. C., Davis, L. L., & Kraemer, H. C. (2011). The role and interpretation of pilot studies in clinical research. *Journal of Psychiatric Research, 45,* 626-629. doi:10.1016/j.jpsychires.2010.10.008

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with Internet use policy from the perspective of rational choice theory. *Decision Support Systems, 48*, 635-645. doi:10.1016/j.dss.2009.12.005

Liptak, A. (2005, July 7). Reporter jailed after refusing to name source. *The New York Times*. Retrieved from http://www.nytimes.com/2005/07/07/politics/07leak.html?pagewanted=all&_r=0

MacCallum, R., Widaman, K., Zhang, S., & Hong, S. (1999). Sample size in factor analysis. *Psychological Methods*, *4*, 84-99. doi:10.1037//1082-989x.4.1.84

Mak, T. (2012). *5 leaks that have Congress steamed*. Retrieved from http://www.politico.com/news/stories/0612/77158.html

McNabb, D. E. (2008). *Research methods in public administration and nonprofit management: Quantitative and qualitative approaches* (2nd ed.). Armonk, NY: M. E. Sharpe.

Mertler, C., & Vannatta, R. (2010). *Advanced and multivariate statistical methods: Practical application and interpretation* (4th ed.). Los Angeles, CA: Pyrzak.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, *1*, 126-139. doi:10.1057/ejis.2009.10

Nagin, D. S., & Paternoster, R. (1991). The preventive effects of the perceived risk of arrest: Testing an expanded conception of deterrence. *Criminology, 29*, 561-561. doi:10.1111/j.1745-9125.1991.tb01080.x

Nagin, D. S., & Paternoster, R. (1994). Personal capital and social control: The deterrence implications of a theory of individual differences in criminal offending. *Criminology*, *32*, 581-581. doi:10.1111/j.1745-9125.1994.tb01166.x

Nagin, D. S., & Pepper, J. (2012). *Deterrence and the death penalty*. Washington, DC: National Academies Press.

Nagin, D. S., & Pogarsky, G. (2001). Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: Theory and evidence. *Criminology*, *39*, 865-892. doi:10.1111/j.1745-9125.2001.tb00943.x

Nagin, D. S., & Pogarsky, G. (2003). An experimental investigation of deterrence: Cheating, self-serving bias, and impulsivity. *Criminology*, *41*, 167-194. doi:10.1111/j.1745-9125.2003.tb00985.x

National Center for Credibility Assessment. (2011). Federal examiner handbook. *Polygraph*, *40*(1), 1-66. Retrieved from http://www.polygraph.org/publications

National Center for Credibility Assessment. (2013a). *Courses offered*. Retrieved from http://www.ncca.mil/courses_offered.htm

National Center for Credibility Assessment. (2013b). *History: The origin and evolution of NCCA*. Retrieved from http://www.ncca.mil/history.htm

National Research Council. (2003). *The polygraph and lie detection*. Washington, DC: National Academies Press.

Nelson, R. (2015). Scientific basis for polygraph testing. *Polygraph*, *44*(1), 28-61. Retrieved from http://www.polygraph.org/publications

Nowlis, S. M., Kahn, B. E., & Dhar, R. (2002). Coping with ambivalence: The effect of removing a neutral option on consumer attitude and preference judgments. *Journal of Consumer Research, 29,* 319-334. doi:10.1086/344431

Office of the Director of National Intelligence. (2012). *Director Clapper announces steps to deter and detect unauthorized disclosures*. Retrieved from http://www.dni.gov/index.php/newsroom/press-releases/96-press-releases-2012/586-director-clapper-announces-steps-to-deter-and-detect-unauthorized-disclosures

Office of the Director of National Intelligence. (2013). *National intelligence program congressional budget justification*. Retrieved from http://fas.org/irp/budget/

Office of the Director of National Intelligence. (2015a). *Conduct of polygraph examinations for personnel security vetting*. Retrieved from http://www.dni.gov/files/documents/ICPG/ICPG%20704.6.pdf

Office of the Director of National Intelligence. (2015b). *America's intelligence community*. Retrieved from http://www.intelligence.gov/files/IC_Overview.pdf

Pallant, J. (2010). *SPSS survival manual* (4th ed.). New York, NY: McGraw-Hill.

Paternoster, R., Saltzman, L., Waldo, G., & Chiricos, T. (1983a). Estimating perceptual stability and deterrent effects: The role of perceived legal punishment in the inhibition of criminal involvement. *Journal of Criminal Law and Criminology, 74*, 270-297. doi: doi:10.2307/1143322

Paternoster, R., Saltzman, L., Waldo, G., & Chiricos, T. (1983b). Perceived risk and social control: Do sanctions really deter? *Law and Society Review*, *17*, 457-479. doi:10.2307/3053589

Paternoster, R., & Simpson, S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law and Society Review*, *30*, 549-583. doi:10.2307/3054128

Peterson, A., Jung, W.-J., & Stanley, H. E. (2008). On the distribution of career longevity and the evolution of home-run prowess in professional baseball. *Europhysics Letters*, *83*, 1-5. doi:10.1209/0295-5075/83/50010

Ponemon Institute. (2011). *Second annual cost of cyber crime study: Benchmark study of U.S. companies*. Retrieved from http://www.hpenterprisesecurity.com/collateral/report/2011_Cost_of_Cyber_Crime_Study_August.pdf

Pozen, D. E. (2013). The leaky leviathan: Why the government condemns and condones unlawful disclosures of information. *Harvard Law Review*, *127*, 512-635 Retrieved from http://harvardlawreview.org/2013/12/the-leaky-leviathan-why-the-government-condemns-and-condones-unlawful-disclosures-of-information/

Puhakainen, P. (2006). *Design theory for information security awareness* (Unpublished doctoral dissertation). University of Oulu, Finland.

Sawyer, A. G. (1982). Statistical power and effect size in consumer research. In A. Mitchell (Ed.), *Advances in consumer research* (pp. 1-7). Ann Abor, MI: Association for Consumer Research.

Schmidt, M. (2013, May 5). Ex-officer for C.I.A. is sentenced in leak case. *The New York Times*. Retrieved from http://www.nytimes.com/2013/01/26/us/ex-officer-for-cia-is-sentenced-in-leak-case.html?_r=0

Schmitt, R. B. (2005, July 7). Journalist jailed for not revealing source to court. *Los Angeles Times*. Retrieved from http://articles.latimes.com/2005/jul/07/nation/na-reporters7

Scott, J. (2000). Rational choice theory. In C. Browning, A. Halchi, & F. Webster (Eds.), *Understanding contemporary society: Theories of the present* (pp. 126-138). Thousand Oaks, CA: Sage.

Siponen, M. T. (2000). A conceptual foundation for organizational IS security awareness. *Information Management and Computer Security*, *8*, 31-41. doi:10.1108/09685220010371394

Siponen, M. T. (2002). On the role of human morality in information system security: From the problems of descriptivism to non-descriptive foundations. In A. Salehnia (Ed.), *Ethical issues of information systems* (pp. 255-271). Hershey, PA: Idea Group.

Stahl, B. (2004). Responsibility for information assurance and privacy: A problem of individual ethics? *Journal of Organizational and End User Computing*, *16*, 59-77. doi:10.4018/joeuc.2004070104

Stat Trek. (2015). *What is cluster sampling*. Retrieved from http://stattrek.com/survey-research/cluster-sampling.aspx

Stevens, J. (1999). *Intermediate statistics* (2nd ed.). Mahwah, NJ: Routledge Academic.

Straub, D. W. (1990). Effective IS aecurity: An empirical study. *Information Systems Research, 1,* 255-276. doi:10.1287/isre.1.3.255

Strelan, P., & Boeckman, R. (2006). Why drug testing in elite sport does not work: Perceptual deterrence theory and the role of personal moral beliefs. *Journal of Applied Social Psychology, 36,* 2909-2934. doi:10.1111/j.0021-9029.2006.00135.x

Suhr, D. (2005). *Principal component analysis vs. exploratory factor analysis*. Retrieved from http://www2.sas.com/proceedings/sugi30/203-30.pdf

Sylvers, P., & Lilienfeld, S. O. (2015). Polygraph analysis. *Salem Press Encyclopedia of Science*, 1-3. Retrieved from http://www.salempress.com/

Tabachnick, B., & Fidell, L. (2012). *Using multivariate statistics* (6th ed.). Boston, MA: Pearson.

Trovillo, P. (1939). A history of lie detection. *Journal of Criminal Law and Criminology, 29,* 848-881. doi:10.2307/1136489

U.S. Army. (1993). *The Army counterintelligence program*. Retrieved from https://fas.org/irp/doddir/army/ar381-20.pdf

U.S. Army. (1995). *Department of the Army polygraph activities*. Retrieved from https://fas.org/irp/doddir/army/ar195-6.pdf

U.S. Army. (2011). *AR 15-6 report - Compromise of classified information to Wikileaks*. Retrieved from http://media.washtimes.com.s3.amazonaws.com/media/misc/2014/10/02/army-regulation-15-6-investigation_wikileaks-ar-15-6-roi-redacted.pdf

U.S. Department of Defense. (1984). *DoD polygraph program*. Retrieved from http://www.fas.org/sgp/othergov/polygraph/dod5210-48.html

U. S. Department of Defense. (2006). *National industrial security program*. Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/522022m.pdf

U. S. Department of Justice Office of Public Affairs. (2012). *U.S. DOJ: Former CIA Officer John Kiriakou charged with disclosing covert officer's identity and other classified information to journalists and lying to CIA's publications review board*. Retrieved from http://www.justice.gov/opa/pr/2012/January/12-ag-083.html

U.S. Department of Labor. (2008). *Fact sheet #36: Employee polygraph protection act of 1988*. Retrieved from http://www.dol.gov/whd/regs/compliance/whdfs36.pdf

U. S. Department of Labor. (2013). *The Employee Polygraph Protection Act (EPPA)*. Retrieved from http://www.dol.gov/compliance/laws/comp-eppa.htm

U.S. Government. (2013). *10 U.S.C § 1564a - Counterintelligence polygraph program*. Retrieved from http://www.law.cornell.edu/uscode/text/10/1564a

United States of America v. Hitselberger, 909 F. Supp. 2d 4 (United States District Court, District of Columbia 2012).

United States v. Manning, (The United States Army First Judicial Circuit 2013).

van Teijlingen, E. R., & Hundley, V. (2001). *The importance of pilot studies*. Retrieved from http://sru.soc.surrey.ac.uk/SRU35.pdf

Vance, A., & Siponen, M. (2012). IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing*, *24,* 21-41. doi:10.4018/joeuc.2012010102

Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. *Computers and Security*, *23,* 191-198. doi:10.1016/j.cose.2004.01.012

Watson, R. (1986). The effectiveness of increases police enforcement as a general deterrent. *Law and Society Review*, *20,* 293-299. doi:10.2307/3053544

Weisburd, D., Waring, E., & Chayet, E. (1995). Specific deterrence in a sample of offenders convicted of white-collar crimes. *Criminology*, *33,* 587-587. doi:10.1111/j.1745-9125.1995.tb01191.x

Wood, P. B., Gove, W. R., Wilson, J. A., & Cochran, J. K. (1997). Nonsocial reinforcement and habitual criminal conduct: An extension of learning theory. *Criminology*, *35,* 335-366. doi:10.1111/j.1745-9125.1997.tb00879.x

Wright, V. (2010). *Deterrence in criminal justice: Evaluating certainty vs. severity of punishment*. Retrieved from http://www.sentencingproject.org/doc/Deterrence%20Briefing%20.pdf

Yiu, D. W., Xu, Y., & Wan, W. P. (2014). The deterrence effects of vicarious punishments on corporate financial fraud. *Organization Science*, *25,* 1549-1571. doi:10.1287/orsc.2014.0904

Young, K. S., & Case, C. J. (2004). Internet abuse in the workplace: New trends in risk management. *Cyberpsychology and Behavior*, *7*, 105-111. doi:10.1089/109493104322820174

Appendix A: Consent Form

CONSENT FORM

You are invited to take part in a research study of Polygraph Deterrence. The researcher is inviting individuals in the following categories:

a. Who have taken a screening polygraph within the last year AND are currently in a position that may require a polygraph test. Being in a position that requires a polygraph is identified by signing a statement of understanding that a person may be required to take a polygraph in the future as part of their job.

b. Who have NOT taken a screening polygraph within the last year and are NOT in a position that may require a polygraph as a condition of employment.

This form is part of a process called "informed consent" to allow you to understand this study before deciding whether to take part.

This study is being conducted by Joshua Cook, a doctoral candidate at Walden University. You may already know or have met Mr. Cook during the course of your work. This study is not related to his current job and your participation in the survey will have no impact on your relationship with Mr. Cook. This study is wholly separate from his role in his current job.

Background Information:
The purpose of this study is to determine deterrence effects of a screening polygraph examination.

Procedures:
If you agree to be in this study, you will be asked to:

- Complete a questionnaire along with a brief statement on your polygraph experience. The questionnaire will take approximately 15 minutes.

Here are some sample questions:
1. As part of a security program, personnel should be subjected to a random polygraph.
Strongly agree Agree Neutral/No Opinion Disagree Strongly disagree
5 4 3 2 1
2. As part of a security program, personnel should be subjected to a mandatory polygraph exam.
Strongly agree Agree Neutral/No Opinion Disagree Strongly disagree
5 4 3 2 1
3. Random polygraph exams can help prevent espionage.
Strongly agree Agree Neutral/No Opinion Disagree Strongly disagree
5 4 3 2 1

Voluntary Nature of the Study:
This study is strictly voluntary. Mr. Cook will be the only researcher involved in this study and he will respect your decision of whether or not you choose to be in the study. No one in the polygraph community will treat you differently if you decline to participate in the study. This study will NOT impact your occupation in the future and it WILL NOT impact your ability to receive a screening polygraph in the future. If you decide to join the study now, you can still change your mind during or after the study. You may stop at any time. The survey is completely anonymous.

Risks and Benefits of Being in the Study:
Being in this type of study involves some minor risk of discomfort, similar to what would be experienced in daily life. An example would be recalling an unpleasant experience during a polygraph examination or being asked to choose between whether or not you agree or disagree with certain policies related to polygraph employment. Being in this study will NOT pose a risk to your safety or wellbeing.

The study is likely beneficial because it will assist in determining the impact having a screening polygraph program is for programs that use a polygraph to protect its proprietary or restricted information. It will also help determine how effective the policy in place is and will help provide a quantitative justification for continuation or change in the polygraph policy currently in place.

Payment:
There will be no payment offered for your voluntary participation.

Privacy:
Any information you provide will be kept confidential and will not be used in any government function. This study is NOT part of any government activity. All surveys will be anonymous and the data collected from the survey will be encrypted and maintained for 5 years, as required by the University. Mr. Cook will not use your information for any other purposes outside the study. He will also remove any identifying information from any information that may indicate the author of a particular survey.

Contacts and Questions:
You may ask any questions you have now. Or if you have questions later, you may contact the researcher via email at Joshua.cook @ waldenu.edu. If you want to talk privately about your rights as a participant, you can call Dr. Leilani Endicott. She is the Walden University representative who can discuss this with you. Her phone number is 1-800-925-3368, extension 1210. Walden University's approval number for this study is 08-13-14-0118381 and it expires on August 12, 2015.
You may print a copy of this questionnaire for your records.
Statement of Consent:

I have read the above information and I feel I understand the study well enough to make a

decision about my involvement. Completing the web link survey indicates I voluntarily consented to the terms described above I understand that I am agreeing to the terms described above.

Appendix B: Questionnaire

Questionnaire

a. Have you taken a screening polygraph examination in the past 1 year? (Yes, see question b) (No, see question c).

b. Approximately when did you take your polygraph exam? (Month/Year)

c. Does your current employment position require you to take a polygraph as a condition of employment? (e.g., you have signed a form stating you might be required to take a polygraph as a condition of employment) (if yes, participant is not eligible. If no, participant is part of no polygraph-treatment group).

d. Are you 18 years old or older (Y/N) What is the month/year of birth?

e. Are you a U.S. person (green card holder/U.S. Citizen) (Y/N).

Survey Definitions

DISCLAIMER: For the purposes of the research, it is assumed that a perception of the polygraph is based on the need to take the polygraph as part of a person's employment. Therefore, the definitions of mandatory and random may not be consistent with the definitions used in actual polygraph programs.

Screening Polygraph: A screening polygraph exam is a generic polygraph examination with broad questions. The screening polygraph exam is non-accusatory and is not prompted by any specific incident or accusation.

Mandatory Polygraph: A polygraph test that is taken on a predictable regular basis, typically conducted on a 5 year basis and called a periodic polygraph test.

Random Polygraph: A polygraph test that is taken on an unpredictable basis. An example of a random polygraph would be a polygraph taken at 12 months within the start of employment, then within 3 years of the last test, then 2 years later. Generally a random polygraph is not conducted in a predictable manner. Random polygraph exams can also be considered aperiodic tests.

Security: Related to the individual responsibilities regarding protection and proper storage of proprietary or classified national defense information. The information is something an organization desires to hold close in order to protect organizational information, trade secrets, national defense information, etc. It is directly related to adherence of proper procedures in order to protect the information and prevent inadvertent or deliberate disclosures to unauthorized personnel.

Espionage: The providing of sensitive information to a competing power regarding organizational information, trade secrets or national defense information by a willing individual in order to give a potential advantage to the competing power. The providing of the sensitive information is often accompanied by reward to the provider of the information, which comes in the form of personal gain.

Leaks: The unauthorized provision of sensitive information to members of the media, often done to damage the reputation of a party privy to the information or to gain an advantage in certain negotiations.

Security program: A series of regulations and rules administered by a group of individuals with power to enforce and recommend sanctions for failure to adhere to regulations and rules. The purpose of the program is to protect sensitive organizational information, and to maintain an organization's competitive edge when dealing with competing organizations.

Deliberate security compromises: The deliberate violation of a security directive or rule, designed to protect a company's information and maintain its competitive edge.

Survey

1. As part of a security program, personnel should be subjected to a RANDOM polygraph exam.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

2. As part of a security program, personnel should be subjected to a MANDATORY polygraph exam.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

3. RANDOM polygraph exams can help prevent espionage.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

4. MANDATORY polygraph exams can help prevent espionage.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

5. MANDATORY polygraph exams can help prevent deliberate security compromises.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

6. RANDOM polygraph exams can help prevent deliberate security compromises.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

7. I adhere more closely to security regulations because I am subjected to a RANDOM polygraph exam on security regulations.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

8. I adhere more closely to security regulation because I am subjected to a MANDATORY polygraph exam on security regulations.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

9. I would adhere more closely to security regulations if I were subjected to a RANDOM polygraph exam.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

10. I would adhere more closely to security regulations if I were subjected to a MANDATORY polygraph exam.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

11. Security will be enhanced if more people were subjected to a RANDOM polygraph exam

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

12. Security will be enhanced if more people were subjected to a MANDATORY polygraph exam

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

13. More frequent polygraph exams can enhance the security of the Department of Defense.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

14. Those subjected to MANDATORY polygraph exams adhere more closely to the security regulations.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

15. Those subjected to RANDOM polygraph exams adhere more closely to the security regulations.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

16. RANDOM polygraph exams can help prevent deliberate security compromises.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

17. MANDATORY polygraph exams can help prevent deliberate security compromises.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

18. Polygraph exams are a necessary part of a security program.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

19. A MANDATORY polygraph exam can help detect deliberate security compromises.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

20. A RANDOM polygraph exam can help detect deliberate security compromises.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

(question not evaluated, used to determine answering bias) -Taking a polygraph examination is an enjoyable experience.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

21. People with a high level security clearance should be given a polygraph exam.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

22. People with a high level security clearance should be subjected to a MANDATORY polygraph exam.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

23. People with a high level security clearance should be subjected to a RANDOM polygraph exam.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

24. MANDATORY polygraph exams can enhance workplace security.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

25. RANDOM polygraph exams can enhance workplace security.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

26. I would commit a security violation even if I was subjected to a polygraph exam.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

(question not evaluated, used to determine answering bias) -The results of a polygraph should not be used when making a security decision.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

27. RANDOM polygraph examinations can help prevent leaks of classified information.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

28. MANDATORY polygraph examinations can help prevent leaks of classified information.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

(question not evaluated, used to determine answering bias) Information on RANDOM polygraph examinations should be excluded from MANDATORY Threat Awareness briefings.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

(question not evaluated, used to determine answering bias) A deliberate security compromise is OK.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

29. I am willing to take a RANDOM polygraph exam as part of a security program.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

30. I am willing to take a MANDATORY polygraph exam in order to enhance a security program.

Strongly agree	Agree	Neutral/No Opinion	Disagree	Strongly disagree
5	4	3	2	1

Appendix C: Survey Factor 1 and 3 *t* Test and Significance

An independent samples *t* test was conducted to assess if there were differences in Factor 1 by group (taken polygraph in the past year: yes vs. no) (alpha = .95). Prior to analysis, the assumption of normality was assessed using a Shapiro-Wilk test. The result of the test was significant, $p < .001$, violating the assumption of normality; however, the *t* test is robust to violations of normality (Howell, 2012). The assumption of equality of variance was assessed using Levene's test. The result of the test was significant, $p = .036$, violating the assumption of equality of variance; therefore, the Welch *t* statistic, which does not assume equality of variance, was used (Stevens, 1999).

The results of the independent sample *t* test were significant, $t(324) = -5.21$, $p < .001$, suggesting that there was a difference on Factor 1 by group. Participants who had not taken a polygraph in the past year scored significantly lower than participants who had taken a polygraph in the past year. According to Cohen (1988), the difference between the two groups was a medium effect size. Results of the independent sample *t* test are presented in Table 1.

Table A1

Independent Sample t Test for Factor 1 by Group (Taken Polygraph: Yes vs. No)

				No		Yes	
Variable	*t*(324)	*p*	*d*	*M*	*SD*	*M*	*SD*
Factor 1	-5.21	.001	0.58	3.60	0.83	4.05	0.71

An independent samples *t* test was conducted to assess if there were differences in Factor 3 group (taken polygraph in the past year: yes vs. no;alpha = .89). Prior to analysis, the assumption of normality was assessed using a Shapiro-Wilk test. The result of the test was significant, $p < .001$, violating the assumption of normality; however, the t-test is robust to violations of normality (Howell, 2010). The assumption of equality of variance was assessed using Levene's test. The result of the test was significant, $p < .001$, violating the assumption of equality of variance; therefore, the Welch *t* statistic, which does not assume equality of variance, was used (Stevens, 1999).

The results of the independent sample *t* test were significant, $t(313) = -9.04$, $p < .001$, suggesting that there was a difference in Factor 3 by group. Participants who had not taken a polygraph in the past year scored significantly lower than participants who had taken a polygraph in the past year. According to Cohen (1988), the difference between the two groups was a large effect size. Results of the independent sample *t* test are presented in Table 2.

Table A2

Independent Sample t Test for Factor 3 by Group (Taken Polygraph: Yes vs. No)

				No		Yes	
Variable	*t*(313)	*p*	*d*	*M*	*SD*	*M*	*SD*
Factor 3	-9.04	.001	0.99	3.52	0.70	4.13	0.51

Appendix D: Frequencies and Percentages for Nominal Variables Combined

Variables	*n*	%
Question 1		
Agree	151	46
Disagree	46	14
Neutral / No Opinion	51	16
Strongly agree	70	21
Strongly disagree	8	2
Question 2		
Agree	121	37
Disagree	54	17
Neutral / No Opinion	50	15
Strongly agree	90	28
Strongly disagree	11	3
Question 3		
Agree	165	51
Disagree	31	10
Neutral / No Opinion	44	13
Strongly agree	79	24
Strongly disagree	7	2
Question 4		
Agree	145	44
Disagree	47	14
Neutral / No Opinion	57	17
Strongly agree	69	21
Strongly disagree	8	2
Question 5		
Agree	153	47
Disagree	43	13
Neutral / No Opinion	45	14
Strongly agree	75	23
Strongly disagree	10	3
Question 6		
Agree	166	51
Disagree	33	10
Neutral / No Opinion	42	13
Strongly agree	77	24
Strongly disagree	8	2

Question 7		
Agree	55	17
Disagree	53	16
Neutral / No Opinion	146	45
Strongly agree	37	11
Strongly disagree	35	11
Question 8		
Agree	60	18
Disagree	50	15
Neutral / No Opinion	140	43
Strongly agree	43	13
Strongly disagree	33	10
Question 9		
Agree	111	34
Disagree	65	20
Neutral / No Opinion	69	21
Strongly agree	56	17
Strongly disagree	25	8
Question 10		
Agree	105	32
Disagree	69	21
Neutral / No Opinion	70	21
Strongly agree	57	17
Strongly disagree	25	8
Question 11		
Agree	169	52
Disagree	33	10
Neutral / No Opinion	52	16
Strongly agree	68	21
Strongly disagree	4	1
Question 12		
Agree	153	47
Disagree	39	12
Neutral / No Opinion	65	20
Strongly agree	63	19
Strongly disagree	6	2
Question 13		
Agree	154	47
Disagree	32	10
Neutral / No Opinion	59	18

Strongly agree	74	23
Strongly disagree	7	2
Question 14		
Agree	139	43
Disagree	35	11
Neutral / No Opinion	83	25
Strongly agree	61	19
Strongly disagree	8	2
Question 15		
Agree	152	47
Disagree	38	12
Neutral / No Opinion	68	21
Strongly agree	62	19
Strongly disagree	6	2
Question 16		
Agree	167	51
Disagree	36	11
Neutral / No Opinion	43	13
Strongly agree	74	23
Strongly disagree	6	2
Question 17		
Agree	163	50
Disagree	39	12
Neutral / No Opinion	49	15
Strongly agree	70	21
Strongly disagree	5	2
Question 18		
Agree	137	42
Disagree	33	10
Neutral / No Opinion	51	16
Strongly agree	96	29
Strongly disagree	9	3
Question 19		
Agree	176	54
Disagree	32	10
Neutral / No Opinion	48	15
Strongly agree	63	19
Strongly disagree	7	2
Question 20		
Agree	171	52

Disagree	30	9
Neutral / No Opinion	47	14
Strongly agree	72	22
Strongly disagree	6	2
Question 21		
Agree	33	10
Disagree	93	29
Neutral / No Opinion	140	43
Strongly agree	9	3
Strongly disagree	51	16
Question 22		
Agree	119	37
Disagree	16	5
Neutral / No Opinion	31	10
Strongly agree	153	47
Strongly disagree	7	2
Question 23		
Agree	111	34
Disagree	20	6
Neutral / No Opinion	48	15
Strongly agree	138	42
Strongly disagree	9	3
Question 24		
Agree	120	37
Disagree	25	8
Neutral / No Opinion	44	13
Strongly agree	128	39
Strongly disagree	9	3
Question 25		
Agree	153	47
Disagree	29	9
Neutral / No Opinion	79	24
Strongly agree	58	18
Strongly disagree	7	2
Question 26		
Agree	156	48
Disagree	31	10
Neutral / No Opinion	58	18
Strongly agree	75	23
Strongly disagree	6	2

Question 27		
Agree	16	5
Disagree	77	24
Neutral / No Opinion	33	10
Strongly agree	4	1
Strongly disagree	196	60
Question 28		
Agree	53	16
Disagree	136	42
Neutral / No Opinion	87	27
Strongly agree	11	3
Strongly disagree	39	12
Question 29		
Agree	163	50
Disagree	41	13
Neutral / No Opinion	49	15
Strongly agree	67	21
Strongly disagree	6	2
Question 30		
Agree	156	48
Disagree	44	13
Neutral / No Opinion	59	18
Strongly agree	63	19
Strongly disagree	4	1
Question 31		
Agree	62	19
Disagree	95	29
Neutral / No Opinion	129	40
Strongly agree	14	4
Strongly disagree	26	8
Question 32		
Agree	12	4
Disagree	50	15
Neutral / No Opinion	21	6
Strongly agree	2	1
Strongly disagree	241	74
Question 33		
Agree	154	47
Disagree	16	5
Neutral / No Opinion	36	11

Strongly agree	107	33
Strongly disagree	13	4
Question 34		
Agree	143	44
Disagree	20	6
Neutral / No Opinion	31	10
Strongly agree	117	36
Strongly disagree	15	5

Note. Due to rounding error, percentages may not add up to 100.

Appendix E: Frequencies and Percentages for Nominal Variables Yes polygraph

Variables	*n*	%
Question 1		
Agree	70	46
Disagree	8	5
Neutral / No Opinion	25	16
Strongly agree	46	30
Strongly disagree	3	2
Question 2		
Agree	58	38
Disagree	6	4
Neutral / No Opinion	20	13
Strongly agree	66	43
Strongly disagree	2	1
Question 3		
Agree	71	47
Disagree	5	3
Neutral / No Opinion	18	12
Strongly agree	57	38
Strongly disagree	1	1
Question 4		
Agree	75	49
Disagree	4	3
Neutral / No Opinion	21	14
Strongly agree	51	34
Strongly disagree	1	1
Question 5		
Agree	72	47
Disagree	3	2
Neutral / No Opinion	19	13
Strongly agree	55	36
Strongly disagree	3	2
Question 6		
Agree	70	46
Disagree	5	3
Neutral / No Opinion	19	13
Strongly agree	56	37
Strongly disagree	2	1
Question 7		

Agree	32	21
Disagree	31	20
Neutral / No Opinion	51	34
Strongly agree	26	17
Strongly disagree	12	8
Question 8		
Agree	36	24
Disagree	27	18
Neutral / No Opinion	45	30
Strongly agree	32	21
Strongly disagree	12	8
Question 9		
Agree	37	24
Disagree	29	19
Neutral / No Opinion	46	30
Strongly agree	30	20
Strongly disagree	10	7
Question 10		
Agree	42	28
Disagree	30	20
Neutral / No Opinion	43	28
Strongly agree	27	18
Strongly disagree	10	7
Question 11		
Agree	71	47
Disagree	8	5
Neutral / No Opinion	26	17
Strongly agree	46	30
Strongly disagree	1	1
Question 12		
Agree	76	50
Disagree	7	5
Neutral / No Opinion	27	18
Strongly agree	40	26
Strongly disagree	2	1
Question 13		
Agree	69	45
Disagree	8	5
Neutral / No Opinion	27	18
Strongly agree	47	31

Strongly disagree	1	1
Question 14		
Agree	67	44
Disagree	12	8
Neutral / No Opinion	36	24
Strongly agree	35	23
Strongly disagree	2	1
Question 15		
Agree	64	42
Disagree	14	9
Neutral / No Opinion	37	24
Strongly agree	36	24
Strongly disagree	1	1
Question 16		
Agree	72	47
Disagree	9	6
Neutral / No Opinion	22	14
Strongly agree	48	32
Strongly disagree	1	1
Question 17		
Agree	77	51
Disagree	9	6
Neutral / No Opinion	19	13
Strongly agree	46	30
Strongly disagree	1	1
Question 18		
Agree	62	41
Disagree	3	2
Neutral / No Opinion	14	9
Strongly agree	72	47
Strongly disagree	1	1
Question 19		
Agree	88	58
Disagree	3	2
Neutral / No Opinion	16	11
Strongly agree	44	29
Strongly disagree	1	1
Question 20		
Agree	76	50
Disagree	5	3

Neutral / No Opinion	20	13
Strongly agree	50	33
Strongly disagree	1	1
Question 21		
Agree	27	18
Disagree	45	30
Neutral / No Opinion	58	38
Strongly agree	8	5
Strongly disagree	14	9
Question 22		
Agree	51	34
Disagree	1	1
Neutral / No Opinion	8	5
Strongly agree	90	59
Strongly disagree	2	1
Question 23		
Agree	49	32
Disagree	3	2
Neutral / No Opinion	12	8
Strongly agree	86	57
Strongly disagree	2	1
Question 24		
Agree	49	32
Disagree	5	3
Neutral / No Opinion	20	13
Strongly agree	75	49
Strongly disagree	3	2
Question 25		
Agree	76	50
Disagree	4	3
Neutral / No Opinion	31	20
Strongly agree	40	26
Strongly disagree	1	1
Question 26		
Agree	70	46
Disagree	6	4
Neutral / No Opinion	27	18
Strongly agree	48	32
Strongly disagree	1	1
Question 27		

Agree	7	5
Disagree	26	17
Neutral / No Opinion	10	7
Strongly agree	2	1
Strongly disagree	107	70
Question 28		
Agree	13	9
Disagree	71	47
Neutral / No Opinion	44	29
Strongly agree	3	2
Strongly disagree	21	14
Question 29		
Agree	76	50
Disagree	9	6
Neutral / No Opinion	22	14
Strongly agree	44	29
Strongly disagree	1	1
Question 30		
Agree	72	47
Disagree	8	5
Neutral / No Opinion	26	17
Strongly agree	45	30
Strongly disagree	1	1
Question 31		
Agree	24	16
Disagree	48	32
Neutral / No Opinion	55	36
Strongly agree	10	7
Strongly disagree	15	10
Question 32		
Agree	4	3
Disagree	13	9
Neutral / No Opinion	2	1
Strongly disagree	133	88
Question 33		
Agree	70	46
Disagree	2	1
Neutral / No Opinion	7	5
Strongly agree	70	46
Strongly disagree	3	2

Question 34		
Agree	65	43
Disagree	2	1
Neutral / No Opinion	3	2
Strongly agree	80	53
Strongly disagree	2	1

Note. Due to rounding error, percentages may not add up to 100.

Appendix F: Frequencies and Percentages for Nominal Variables No Polygraph Group

Variables	*n*	%
Question 1		
Agree	81	47
Disagree	38	22
Neutral / No Opinion	26	15
Strongly agree	24	14
Strongly disagree	5	3
Question 2		
Agree	63	36
Disagree	48	28
Neutral / No Opinion	30	17
Strongly agree	24	14
Strongly disagree	9	5
Question 3		
Agree	94	54
Disagree	26	15
Neutral / No Opinion	26	15
Strongly agree	22	13
Strongly disagree	6	3
Question 4		
Agree	70	40
Disagree	43	25
Neutral / No Opinion	36	21
Strongly agree	18	10
Strongly disagree	7	4
Question 5		
Agree	81	47
Disagree	40	23
Neutral / No Opinion	26	15
Strongly agree	20	11
Strongly disagree	7	4
Question 6		
Agree	96	55
Disagree	28	16
Neutral / No Opinion	23	13
Strongly agree	21	12
Strongly disagree	6	3

Question 7		
Agree	23	13
Disagree	22	13
Neutral / No Opinion	95	55
Strongly agree	11	6
Strongly disagree	23	13
Question 8		
Agree	24	14
Disagree	23	13
Neutral / No Opinion	95	55
Strongly agree	11	6
Strongly disagree	21	12
Question 9		
Agree	74	43
Disagree	36	21
Neutral / No Opinion	23	13
Strongly agree	26	15
Strongly disagree	15	9
Question 10		
Agree	63	36
Disagree	39	22
Neutral / No Opinion	27	16
Strongly agree	30	17
Strongly disagree	15	9
Question 11		
Agree	98	56
Disagree	25	14
Neutral / No Opinion	26	15
Strongly agree	22	13
Strongly disagree	3	2
Question 12		
Agree	77	44
Disagree	32	18
Neutral / No Opinion	38	22
Strongly agree	23	13
Strongly disagree	4	2
Question 13		
Agree	85	49
Disagree	24	14
Neutral / No Opinion	32	18

Strongly agree	27	16
Strongly disagree	6	3
Question 14		
Agree	72	41
Disagree	23	13
Neutral / No Opinion	47	27
Strongly agree	26	15
Strongly disagree	6	3
Question 15		
Agree	88	51
Disagree	24	14
Neutral / No Opinion	31	18
Strongly agree	26	15
Strongly disagree	5	3
Question 16		
Agree	95	55
Disagree	27	16
Neutral / No Opinion	21	12
Strongly agree	26	15
Strongly disagree	5	3
Question 17		
Agree	86	49
Disagree	30	17
Neutral / No Opinion	30	17
Strongly agree	24	14
Strongly disagree	4	2
Question 18		
Agree	75	43
Disagree	30	17
Neutral / No Opinion	37	21
Strongly agree	24	14
Strongly disagree	8	5
Question 19		
Agree	88	51
Disagree	29	17
Neutral / No Opinion	32	18
Strongly agree	19	11
Strongly disagree	6	3
Question 20		
Agree	95	55

Disagree	25	14
Neutral / No Opinion	27	16
Strongly agree	22	13
Strongly disagree	5	3
Question 21		
Agree	6	3
Disagree	48	28
Neutral / No Opinion	82	47
Strongly agree	1	1
Strongly disagree	37	21
Question 22		
Agree	68	39
Disagree	15	9
Neutral / No Opinion	23	13
Strongly agree	63	36
Strongly disagree	5	3
Question 23		
Agree	62	36
Disagree	17	10
Neutral / No Opinion	36	21
Strongly agree	52	30
Strongly disagree	7	4
Question 24		
Agree	71	41
Disagree	20	11
Neutral / No Opinion	24	14
Strongly agree	53	30
Strongly disagree	6	3
Question 25		
Agree	77	44
Disagree	25	14
Neutral / No Opinion	48	28
Strongly agree	18	10
Strongly disagree	6	3
Question 26		
Agree	86	49
Disagree	25	14
Neutral / No Opinion	31	18
Strongly agree	27	16
Strongly disagree	5	3

Question 27		
Agree	9	5
Disagree	51	29
Neutral / No Opinion	23	13
Strongly agree	2	1
Strongly disagree	89	51
Question 28		
Agree	40	23
Disagree	65	37
Neutral / No Opinion	43	25
Strongly agree	8	5
Strongly disagree	18	10
Question 29		
Agree	87	50
Disagree	32	18
Neutral / No Opinion	27	16
Strongly agree	23	13
Strongly disagree	5	3
Question 30		
Agree	84	48
Disagree	36	21
Neutral / No Opinion	33	19
Strongly agree	18	10
Strongly disagree	3	2
Question 31		
Agree	38	22
Disagree	47	27
Neutral / No Opinion	74	43
Strongly agree	4	2
Strongly disagree	11	6
Question 32		
Agree	8	5
Disagree	37	21
Neutral / No Opinion	19	11
Strongly agree	2	1
Strongly disagree	108	62
Question 33		
Agree	84	48
Disagree	14	8
Neutral / No Opinion	29	17

Strongly agree	37	21
Strongly disagree	10	6
Question 34		
Agree	78	45
Disagree	18	10
Neutral / No Opinion	28	16
Strongly agree	37	21
Strongly disagree	13	7

Note. Due to rounding error, percentages may not add up to 100.