11-2-2020

A Phenomenological Analysis of Information Security Reporting: A Paradoxical Perspective

Robin L. Moore
Georgia State University

PERMISSION TO BORROW

In presenting this dissertation as a partial fulfillment of the requirements for an advanced degree from Georgia State University, I agree that the Library of the University shall make it available for inspection and circulation in accordance with its regulations governing materials of this type. I agree that permission to quote from, copy from, or publish this dissertation may be granted by the author or, in his absence, the professor under whose direction it was written or, in his absence, by the Dean of the Robinson College of Business. Such quoting, copying, or publishing must be solely for scholarly purposes and must not involve potential financial gain. It is understood that any copying from or publication of this dissertation that involves potential gain will not be allowed without written permission of the author.

Robin Layne Moore

NOTICE TO BORROWERS

All dissertations deposited in the Georgia State University Library must be used only in accordance with the stipulations prescribed by the author in the preceding statement.

The author of this dissertation is:

Robin Layne Moore
J. Mack Robinson College of Business
Georgia State University
Tower Place 200, Suite 500
3348 Peachtree Road, NE
Atlanta, GA 30326

The director of this dissertation is:

Dr. Lars Mathiassen
Georgia Research Alliance Eminent Scholar
J. Mack Robinson College of Business
Georgia State University
Tower Place 200, Suite 500
3348 Peachtree Road, NE
Atlanta, GA 30326

A PHENOMENOLOGICAL ANALYSIS OF INFORMATION SECURITY REPORTING: A PARADOXICAL PERSPECTIVE

By

Robin Layne Moore

A Dissertation Submitted in Partial Fulfillment of the Requirements for the Degree Of

Doctorate in Business Administration

In the Robinson College of Business

Of

Georgia State University

GEORGIA STATE UNIVERSITY

ROBINSON COLLEGE OF BUSINESS

2020

ACCEPTANCE

This dissertation was prepared under the direction of Robin Layne Moore's Dissertation Committee. It has been approved and accepted by all members of that committee, and it has been accepted in partial fulfillment of the requirements for the degree of Doctoral of Philosophy in Business Administration in the J. Mack Robinson College of Business of Georgia State University.

Richard Phillips, Ph.D., Dean

DISSERTATION COMMITTEE

Lars Mathiassen, Ph.D. (Chair)

Richard Baskerville, Ph.D.

Karen Loch, Ph.D.

DEDICATION

To my parents Tracy and Nancy Moore, brothers Adam, Cody, Dennis, and sister Nicole. Thank you for instilling in me the values which fuel my curiosity of life and the desire to understand the people in it and how they interact. Tara Moore, my wife, thank you for supporting me in our marriage and all the long hours I spent in research. Finally, my children, Garrett, Tyler, and Bret, thank you for enduring all the hours I missed with you as I worked on research, attended class, or otherwise did not spend it with you. It was a calculated risk that I pray you will understand as you get older. To anyone who has experienced inequality whether it be by your skin color or financial misfortune, stay focused on your goals, trust yourself to overcome, and learn to depend on yourself; you can achieve anything you set your mind to.

ACKNOWLEDGEMENTS

To all the esteemed professors, advisors, and administrative staff I have had the privilege of learning from since joining the Executive Doctorate in Business Administration program. A truly heartfelt thank you.

A special thank you goes to Dr. Lars Mathiassen for providing consistent and rigorous guidance along this journey. I am a better researcher today thanks to your dedication to the field.

Table of Contents

ABSTRACT

A Phenomenological Analysis of Information Security Reporting: A Paradoxical Perspective

BY

Robin Layne Moore

October 2020

Committee Chair: Dr. Lars Mathiassen

Major Academic Unit: Doctor of Business Administration

Current information security research has focused on security threats, prevention of incidents, and federal regulations for reporting incidents. However, we know little about how the behavior of information security professionals impacts security. Against this backdrop, this dissertation seeks to understand the drivers of tensions that information security professionals encounter in the performance of their job functions, which result in paradoxical tensions while reporting on the security of organizational assets. The findings of this study reveal how information security professionals respond to inherent tensions as they become salient, and how these salient tensions often become paradoxical in nature as they are dealt with as part of a security professional's everyday lived experience. The findings highlight the actions undertaken by security professionals to resolve these paradoxical tensions and, in doing so, often engage in deviant behaviors that are contrary to organizational policy and industry or governmental

regulations. These findings thus allow for an improved understanding of the motivations of an individual and assist with the creation of policies and management oversight activities that are intended to reduce the likelihood of information security professionals becoming insider threats to their organizations. To that end, an analytical framing combining paradox theory and deterrence theory as complementary theoretical lenses was adopted in this study. Following an interpretive phenomenological analysis methodology, a series of three in-depth interviews, each with eight information security professionals, was conducted. This methodological approach helped the participants to reflect on the drivers of tensions that they perceived as part of their lived experiences. The participants were selected from a range of industries and across a wide spectrum of experiences to capture a broad diversity of lived experiences. Hence, by determining how the drivers of tensions lead to paradoxical tensions that impact or guide the motivations and behaviors of information security professionals responsible for security reporting, the study seeks to contribute to behavioral information security knowledge in the areas of improvement of information security compliance, separation of insider deviant behavior from insider misbehavior, and understanding insider deviant behavior under duress.

Index Terms: Paradox Theory, Neutralization Techniques, Insider Threat, Deviant Behavior, Deviant Behavior Under Duress, Deterrence Theory, Drivers of Tension, Behavioral Information Security, Behavioral InfoSec, Insider Deviant Behavior, Insider Misbehavior, Paradoxical Tensions, Security Professional, Information Security

INTRODUCTION

Information security reporting is important to most organizations. It covers a wide range of security areas such as network security, physical security, vendor risk management, application security, and penetration testing, to name a few. Information security professionals are responsible for ensuring that organizational users comply with security requirements, gather and secure information, investigate and help to recover from security incidents, configure and manage security equipment, and design and monitor security controls, along with many other responsibilities (Lee et al., 2010). The current study focuses on those information security professionals who are responsible for generating information security reports. Information security reports, which can be internal or external to an organization, are produced by information security professionals who are either internal or external to an organization as members of security teams. Both teams are insiders with privileged access to data and assets within the security perimeter of an organization. Information security professionals who are external to an organization are typically members of teams that are hired to perform a service for the organization, for a limited time, and for specific reasons such as scanning software for vulnerabilities or probing a network for security breaches. By contrast, internal security teams engage in the regular and ongoing security reporting for the organization. These external security professionals, who normally serve as external auditors, are privy to security information that is not released to anyone except the organization (Blakley, et al., 2001). These external security reports contain information that is pertinent to vulnerabilities or weaknesses within an organization; hence, the impact on the organization is often greater than reports created by internal teams. Current research on information security reporting is focused on the reporting requirements for incidents that are detected (Ahmad, et al, 2015; Tøndel, et al., 2014; Wiant, 2005), whereas security reporting to

prevent incidents has been largely ignored. This gap in research on information security reporting by information security professionals is the main focus of this study.

Information security professionals perform duties requiring them to be cautious by nature as they work to protect the information within an organization. Such abundance of caution reduces their likelihood of engaging with researchers seeking to improve the understanding of the behaviors of these professionals. The main researcher in this study is an embedded information security professional with over a decade of experience in the information security field covering several security reporting areas, including physical security, vendor risk management, application security, network security, and static code analysis. In addition to the researcher's experience in the information security field, the researcher also has several years of experience as a director on the board of a well-known information security professional association. This experience and leadership in the information security field served to gain access to the information security professionals who are less likely to speak to a researcher who is not embedded in the information security industry. Having a shared experience and knowledge of the field allowed for the recruitment of study participants and for them to provide the details of their experiences in information security reporting to which most researchers would not have had access.

The importance of information security reporting cannot be understated with the information from security reports being used by organizations to determine what and where the security issues are in order to allocate resources for mitigating these security issues. Security reporting is often an automated process, but a human element must always be present. The reason is that automated security reports do not account for mitigating security controls that may reduce or eliminate a security issue, or false positives that are security issues that are reporting incorrectly and must be manually reviewed and removed from the final security report. However, these

information security reports are often manipulated before the final report is presented to the organization's executives. The reasons why these information security professionals alter or manipulate the reports include unethical security cultures, fear of management's reaction to the report results, tight deadlines or poorly scoped engagements, lack of experience, team politics, and coercion by management. The main researcher of this study first learned of information security reports being manipulated by information security professionals during his career in the information security field. This factor was the impetus for undertaking this study to enhance the understanding of the motivations that result in the manipulation of the information security reports. Furthermore, the tensions and the behaviors that information security reporting induces are addressed in this study.

Answering a call for the future direction of behavioral information security research in the areas of the improvement of information security compliance and the separation of insider deviant behavior from insider misbehavior (Crossler et al., 2013), the present study contributes to both areas of concern by conducting a phenomenological analysis of information security professionals with experience in security reporting. As previously stated, information security professionals have an important role in an organization's security, and they are privy to insider knowledge such as vulnerabilities and weaknesses in security. Access to this information places them in a position to be able to cause considerably more damage than a non-security user inside the organization. However, these information security professionals must deal with and overcome the same issues as the non-security users against whom they defend. As the non-security users within an organization can commit non-malicious mistakes or perform deviant acts leading to security incidents, information security professionals can similarly do so. Everyday tensions such as work–life balance, arguments with a coworker or a spouse, fear of management, or disagreements with

a supervisor that engender mistakes or deviant behaviors are not limited to non-security professionals. These tensions must be resolved; however, in resolving those tensions, new ones emerge (Lewis, 2000). In dealing with these tensions, the motivations of individuals lead to their behaviors. To study these tensions and how information security professionals resolve them, we employ paradox theory to provide a paradoxical perspective of information security reporting by security professionals. Paradox theory considers interdependent elements that simultaneously support and oppose each other (Faems & Filatotchev, 2018). These elements are inherent in life and manifest as competing tensions that individuals navigate daily with little or no conscious effort. However, these competing tensions guide the actions and perceptions of how individuals behave. This study shows how these paradoxical tensions guide the actions of information security professionals who are responsible for information security reporting.

To understand the lived experiences of information security professionals and the meanings developed from these complex interactions as they engage in the act of security reporting, a multi-case study was conducted, which allowed for deep and meaningful insights to be drawn from the analysis of the contradictory nature of the paradoxical tensions that information security professionals encounter when generating information security reports (Eisenhardt, 1998). Dealing with tensions is a part of everyone's life. Such tensions are rarely given much thought; instead they are filed away in our memories as common occurrences. The uncovering of these tensions and reflecting on them in a manner that guides a study participant to engage in meaning making require more than one conversation. As such, a series of three in-depth interviews was conducted and evaluated using an interpretive phenomenological analysis (IPA) methodology. Phenomenological analysis is designed to understand the complex meanings that individuals develop by reflecting on their lived experiences (Alase, 2017). The current study consists of eight participants, each a

unique case as each has a different perspective on their lived experiences. By analyzing these eight cases using an interpretive phenomenological analysis method, we are able to discover the gestalt of tensions encountered by information security professionals in security reporting activities.

The research design summary is provided in Figure 1. The remainder of the study is organized into several chapters. Chapter I covers behavioral information security and the two main areas to which this study is expected to contribute. Chapter II includes paradox theory and complementary theories. Chapter III provides details into the research methodology used for this study. Chapter IV outlines the results that the study generated. Finally, Chapter V concludes the paper; it covers a discussion of the results, contributions to practice and theory, limitations of the study, and suggestions for future research.

Figure 1
Research Design Summary – ***Adapted from Mathiassen (2017)***

Component	Definition	Details
P	The problem setting represents people's concerns in a real-world problematic situation.	Information security professionals responsible for security reporting play an important role in the security of an organization while facing the same tensions as non-security users. In managing these tensions, security professionals develop a sense of meaning that leads to their motivations and behaviors. These tensions often create new tensions as they are resolved, making them difficult to manage and increasing the likelihood that they will result in insider deviant behaviors.
A	The area of concern represents a body of knowledge within the literature that relates to the problem setting.	Information security reporting has been empirically studied with regard to incident handling and governmental regulations. However, little research has been conducted to investigate the motivations and behaviors of information security professionals who are responsible for generating the information security reports on which organizations rely.

F	The conceptual framing helps to structure the analysis of data to answer the research question. FA draws upon concepts from the areas of concern, whereas FI is independent of area of concern.	Both paradox theory and attribution theory are used in this study, and this combination constitutes the conceptual framing of the area of concern.
M	The adopted methods of empirical inquiry.	Using a multi-case study format that employs both literal and theoretical replication logic, this study adopts an interpretive phenomenological approach to analyze the meanings that the participants develop from reflecting on their lived experiences in security reporting. A series of three interviews was developed to guide each participant in the reflection process. Each interview was designed to bracket the field of inquiry to the specific area of interest, that is, information security reporting.
RQ	The research question relates to the problem setting; it opens the research into the area of concern and helps to ensure that the research design is coherent and consistent.	How do paradoxical tensions impact or guide the motivations and behaviors of information security professionals who are responsible for security reporting?
C	The contributions to the problem setting and area of concern and possibly to conceptual framework and method.	This study is expected to contribute to behavioral information security knowledge as follows: • Improving information security compliance by demonstrating the behaviors in which information security professionals engage • Increasing the body of knowledge in the area of paradox theory by demonstrating the paradoxical tensions that information security professionals encounter, which affect security reporting • Distinguishing insider deviant behavior from insider misbehavior to include the conceptualization of a new neutralization technique used by security professionals who engage in deviant behavior under duress

CHAPTER I. **BEHAVIORAL INFORMATION SECURITY**

In the insider threat report issued by the Cybersecurity Insiders in 2020, 68% of organizations indicated that they are vulnerable to insider attacks and 63% of organizations consider privileged IT users as their greatest insider security risk (Cybersecurity Insiders, 2019). Understanding the motivations of these insider threats is the focus of behavioral information security. The extant research largely focuses on the technical challenges to information security (Crossler et al., 2013), whereas studies on behavioral information security emphasize the understanding of the individuals' behavior as it relates to information security. In their paper *Future directions for behavioral information security research*, Crossler et al. (2013) calls for researchers to explore four areas of behavioral information security, namely cross-cultural behavioral issues, data collection and measurement issues, improvement of information security compliance, and separation of insider deviant behavior from insider misbehavior. Much of the literature focuses on insiders as the average user of technology who either have or had a legitimate right to access organizational resources (Elifoglu et al., 2018). The current study focuses on the last two of these areas, with emphasis on information security professionals as insiders.

I.1 Improving Information Security Compliance

Behavioral approaches that seek to understand and motivate compliance in information systems are drawn from criminology and psychology to include neutralization techniques, protection motivation theory, and deterrence Theory (Vance et al., 2012). Deterrence theory employs the usage of sanctions to motivate an individual to avoid deviant behavior through the use of fear of those sanctions (Siponen et al., 2010; Straub, 1990; Workman & Gathegi, 2007). To ensure that sanctions are effective, the organization must clarify to the personnel that the detection of their non-compliance will prompt the quick and severe application of the sanctions (Siponen et

al., 2010). As it relates to information security, an example of a sanction is the potential for administrative actions up to and including termination for non-compliance with a security policy. The central tenet of deterrence theory is that an individual will avoid deviant behavior to avert the potential punishment; furthermore, it is predicated on two components, namely the sanction or penalty and the likelihood of being caught (Straub, 1990).

Despite the use of deterrence theory to employ sanctions in the development and deployment of information security polices, deviant non-compliance is still an issue with personnel employing other techniques to avoid or rationalize their non-compliance with security policies (Siponen & Vance, 2010). Neutralization techniques were first developed by Sykes and Matza in 1957 to explain the ability of individuals to rationalize their deviant behavior. Sykes and Matza outlined five major types of neutralization techniques employed by individuals to rationalize their behavior, namely "denial of responsibility", "denial of injury", "denial of the victim", "condemnation of the condemners", and "appeal to higher loyalties" (Sykes & Matza, 1957). Two new major types were later added to the original five. The first new type emerged 17 years after Sykes and Matza's original five, as Carl Klockars added the "metaphor of the ledger" in his book *The Professional Fence* (Klockars, 1975). The final major type was added seven years following that of Klockars when W. William Minor included the "defense of necessity" in the list of neutralization techniques (Minor, 1981). We will not expand on the entire list of neutralization techniques because they only serve to highlight the argument that the use of deterrents or sanctions is insufficient to motivate individuals to avoid deviant behavior in compliance with information security policies. However, we will highlight the newest neutralization technique to be added to the list because it is important to the separation of insider deviant behavior from insider misbehavior. The defense of necessity is employed when individuals perceive their actions as

necessary even when the act is considered deviant or morally wrong (Minor, 1981). Furthermore, the defense of necessity is often employed in minor ways such as justifying the act of speeding because a person is running late. By employing this neutralization technique, individuals can release themselves from feeling guilty of the deviant behavior by justifying it as necessary to avoid the harsher punishment for being late. Notably, all seven neutralization techniques are employed as internal rationalizations to justify deviant behaviors, and they are applicable to both insider deviant behavior and insider misbehavior.

I.2 Distinguishing Insider Deviant Behavior from Insider Misbehavior

The separation of insiders who act in a deviant manner from those who misbehave is a matter of intent by the individual, whereby those who overtly commit to non-compliance such as accessing data or intentionally planting malware are different from the ones who write their passwords on a sticky note and leave it on their desk (Crossler et al., 2013). Insider deviant behavior is understood to be intentional in nature, and it typically involves some benefit such as the monetary gain for selling proprietary secrets or sabotaging organizational systems or data as a form of hacktivism. This insider deviant behavior is likely to cause repercussions on the organization, such as reputational damage due to breach notification requirements or the loss of market share to competitors from the release of intellectual property (Crossler et al., 2013). Insider misbehavior may still have a significant impact on the organization; however, the intent is not to inflict harm, as is the case with insider deviant behavior. An example of this situation may be the accidental setting of a “public” flag on an Amazon S3 bucket containing non-public information, resulting in the data being accessible to anyone outside of the organization. Although unintentional, this misbehavior may result in a data breach similar to the one caused by the deliberate actions of an insider intending to harm the organization. Insider misbehavior typically

causes a weakness in organizational security, thereby allowing for another actor to exploit this weakness though not directly committed by the insider (Crossler et al., 2013).

As their role relates to information security reporting, information security professionals often experience many justifiable reasons for altering an information security report, which would not qualify as a deviant behavior. For instance, information security professionals may be ordered by their manager to alter a security report to reduce a security finding because it is a false positive so as not to create false findings in the report, or because a mitigating control is in place. However, when ordered to act in a deviant manner, these professionals are faced with two competing requirements. They must either do what they have been ordered to do by their manager or comply with the organizational security policy requirements. The war between these two requirements is a latent tension and in being forced to directly deal with this latent tension, it becomes salient and requires a resolution be sought; to the individuals, they perceive themselves as not having a good option. The security policy may state that altering a report in a deviant manner is grounds for termination, whereas not doing so may also result in the potential threat of reprisal from the manager who gave the order. This study views this type of situation as a paradoxical tension. In the next section, paradox theory along with complementary theories are explored.

CHAPTER II. **PARADOX THEORY**

II.1 Paradox Theory

According to Marianne Lewis (2000), paradoxes consist of three characteristics. Paradoxes may constitute a contradictory yet interrelated perspective, feeling, demand or practice, and they are created by actors as they make sense of the intricate and changing world by simplifying the perceived reality into an either/or distinction that simplifies the complex world of reality; furthermore, paradoxes are realized through self-reflection, often simultaneously revealing the absurd and irrational existence of opposites (Lewis, 2000). Paradoxical tensions represent a defining characteristic of a paradox, which may be self-referential loops, mixed messages, and system contradictions (Lewis, 2000; Putnam, 1986). Additionally, paradoxical tensions persist over time, forcing a reflection back on the tensions as they are resolved and thus developing into entirely new tensions that must again be addressed. This process of resolving and creating new tensions causes difficulty in effectively dealing with the tensions (Lewis, 2000; Putnam et al., 2016). Groups such as information security teams are inherently paradoxical, as individuals experience and make sense of the contradictory actions, rules, and instructions that coexist within the group (Smith & Berg, 1997). As individuals define themselves within a group, they create boundaries that delineate their self and the group or team; additionally, they demarcate the boundaries between the group and outside groups such as a group of information security professionals and non-security users creating systems that are inherently paradoxical (Smith & Lewis, 2011). These inherently paradoxical groups or systems create paradoxical tensions.

Putnam et al. (2016) define tensions as “stress, anxiety, discomfort, or tightness in making choices and moving forward in organizational situations” (Putnam et al., 2016, p. 68). Tensions are latent at first, being dormant or ignored, but become salient in specific situations as they

manifest in particular ways, becoming observable and triggering actors to respond (Smith & Lewis, 2011). Relating these tensions to information security professionals as they engage in security reporting, they deal with stress such as unethical instructions, unethical security culture within the organization, tight deadlines, ambiguous instructions, a demanding boss, team politics, and even coercion by management. Such tensions are latent until some action or event forces the information security professional to focus on them, bringing them to salience. Some examples of latent tensions becoming salient for an information security professional include discomfort in making decisions due to conflicting demands given by a manager, a lack of skills, and a superior's demand for actions that are deviant in nature, such as making an individual perform deviant acts that they would not otherwise perform through the use of fear, coercion, or force. How individuals deal with these salient tensions is guided by their perceptions, behaviors, and actions (Ajzen, 1991). Hence, tensions may be responded to in several different ways such as splitting, projecting, repressing, or withdrawal. When the response is splitting, an individual chooses one pole of a tension over the other, further polarizing the contradictions and possibly creating subgroups or social divides (Lewis, 2000). These subgroups subsequently form a we–them distinction such as a group of information security professionals who are told to alter a security report for it to show what management wants it to show, but this group distances itself from the management group as a means of bringing attention to the tension between the two groups (Smith & Berg, 1997). This type of response neither eliminates or resolves the tensions nor overcomes the underlying issue of false reporting to the organization. Projecting is a response whereby a third party is engaged, such as shifting responsibility for the tension to the human resources (HR) department (Putnam et al, 2016) or projecting the blame onto management (Lewis, 2000). This type of response can engage other actors to aid in resolving the tension, such as the HR department making changes to policy

or practices that resolve the tension. However, those same actors may also increase the tension, such as management deciding not to take any action. Using the example of the information security team being ordered to generate false reports, if the management were made aware of the issue but took no action, then the tension felt by the team members might intensify because they see no alternatives. Repression is a response of denial whereby an individual denies the existence of the paradoxical tension and any subsequent tensions (Jarzabkowski & Lê, 2016). This response may be an information security professional denying involvement in any wrongdoing such as the generation of a false security report. This response may be in conjunction with acts of projecting, such as denying responsibility and projecting all the blame on the management who ordered the report to be falsified. Another example would be information security professionals denying any part in a deviant behavior because they acted under duress, such as a manager ordering them to commit some insider deviant act or face termination if they refuse to comply. The fear of termination is a duress condition in which the individual may fear the termination more than committing the insider deviant act itself. An individual may also respond by withdrawing from the salient tension, such as seeking other employment (Putnam et al., 2016). If other responses have failed to resolve the tension or potentially intensified the tension, the response may be to withdraw from it. If an information security team who has been given instructions to alter security reports and has attempted to resolve the tension by speaking to management, yet no resolution was generated, then the team members may elect to seek other employment. This response resolves the salient tension for the individuals as they remove themselves from the organization, but it does not resolve the underlying latent tension for the organization that will continue to generate false security reports.

By guiding the participant in the reflection on such paradoxical situations, the study was able to uncover the absurd and irrational opposites as they are perceived by individuals and the way they have simplified the complex world into straightforward, clearly defined either–or constructs (Lewis, 2000; Lewis & Smith, 2014; Schad et al., 2016). The present study focuses on understanding these tensions and the related behaviors through the lenses of the three characteristics of a paradox as defined by Lewis (2000).

An additional important aspect pertains to what tensions are not. Paradoxical research has used many terms to relate to the tensions inherent in paradox theory. These terms include dualism, duality, contradictions, and dialectics. Dualism typically has a clear contrast with well-defined boundaries that neither overlap nor share a middle ground (Farjoun, 2010). Dualities exist within a whole, but they occur as opposites that create disagreement with the external boundary creating synergy within the whole (Smith & Lewis, 2011). Contradictions are mutually exclusive and interdependent bipolar opposites that may define or even negate each other (Putnam et al., 2016). Finally, dialectics are opposite but interdependent forces that act on each other, constantly sharing the roles of thesis and antithesis as they interact with each other (Putnam et al., 2016; Smith & Lewis, 2011).

Paradoxes have been widely studied in many fields and over several decades. Popular topics for paradoxical studies include organizational paradoxes such as digital technology renewal or transformation (Leonard-Barton, 1992; Wimelius et al., 2020), innovation and reform in telehealth (Cho et al., 2009; Singh et al., 2010; Tracy et al., 2008), stability and innovation (Farjoun, 2010; Tilson et al., 2012), and institutional change (Ford & Ford, 1994; Seo & Creed, 2002). Other studies on paradoxes analyze individuals such as senior leaders' dynamic decision making (Calabretta et al., 2016; Denison et al., 1995; Smith, 2014) and leadership resistance to

change (Ford, et al., 2008; Kan & Parry, 2004). Despite the amount of excellent studies on paradoxes at both the organizational and individual levels, research in the realm of information security professionals remains scant. Given the importance and role of information security professionals in the security of organizations, I thus focus the research on these individuals to increase the understanding of the paradoxical tensions they face and, in doing so, expand the academic knowledge in the area of paradoxical research.

II.2 Complementary theory

Attribution theory explains an individual's perceived relationship between the cause and the outcome of an issue, with issues being either internal or external to the individual (Munton et al., 1999; Park et al., 2008). External attribution assigns causality to factors such as situations or actors, whereas internal attribution ascribes causation that is internal to the individual; furthermore, how individuals perceive these internal and external attributes affect their behavior (Park et al., 2008).

Using attribution theory as the theoretical background, the mum effect explains that an individual's desire to report bad news is influenced by two factors, namely fault responsibility and time urgency (Park et al., 2008). Fault responsibility is the impact that the fear of being responsible for an undesirable outcome will have on the individual's desire to report. The less the individuals perceives themselves as responsible, the more likely they are to report; meanwhile, the inverse is true: the more they perceive themselves as responsible, the less likely they are to report (Park et al., 2008). This aspect is an important complementary factor to paradoxical tensions in that the more responsible the individuals perceive themselves responsible for an outcome, the greater the tension will be perceived. As it relates to information security professionals, the perception of responsibility is due to the belief in management holding them responsible for the results of a

security report. Through management's attribution of accountability to information security professionals, the latter perceive an inheritance of responsibility. The time urgency factor again affects the behavior of individuals as they perceive the relative time before an action has consequences; that is, the less time individuals have, the more likely they are to report and inversely, the more time they have, the less likely they are to report (Park et al., 2008). With regard to paradoxical tensions, as an individual perceives the relative amount of time before actions will have consequences, the less strength one tension will have over another; furthermore, as the time moves closer to the potential consequences, the stronger the tensions will act on the individual.

CHAPTER III. **METHODOLOGY**

Interpretive research helps to increase the understanding of the thoughts and meanings that individuals give to their lived experiences by producing profound insights; meanwhile, phenomenology provides the researcher with the ability to see into the world of the study participants as they experienced it (Klein & Myers, 1999). Phenomenology consists of two main branches, namely the interpretive, also known as hermeneutic, and the descriptive (Jackson et al., 2018). Both methods seek to understand the lived experiences of the participants; however, interpretive phenomenology assumes that the individuals under study have assigned meaning to their lived experiences through artifacts such as language, consciousness, and other social constructs, and it seeks to understand how the participants have assigned meaning to those lived experiences (Boland 1985, 1991; Klein & Myers, 1999; Orlikowski and Baroudi 1991).

The current study uses a series of in-depth interviews with eight participants, each of whom is interviewed thrice, thus forming eight individual case studies. The aim of this study is to explain how paradoxical tensions affect the security reporting of information security professionals; hence, the use of a case study methodology is the appropriate vehicle (Yin, 2018, p. 3).

The remainder of this chapter is structured into several sections. First, the case study design is explained in the first section; this section also presents the rationale for employing a multi-case design and for using the replication logic in the selection of participants. The data collection is outlined in the next section; this section also provides an explanation of the purpose of the three-interview format and the type and structure of the interviews, along with samples of the interview questions. Finally, the third section concludes with the evaluation of the data, covering the use of the interpretive phenomenological analysis as well as the process utilized for developing the results of the study.

III.1 Multi-case Study

An interpretive phenomenological analysis (IPA) methodology was used in this study to understand the complex meanings that participants have developed from reflecting on their own lived experiences (Alase, 2017). The information security professional represented the unit of analysis for the present study; the purpose of the analysis is to comprehend the individuals' meanings developed after reflecting on their role as it relates to security reporting. All the participants are employed in an information security role, and they had one or more previous experiences in an information security role at another organization prior to their current role. This factor provided a homogenous pool of experience to draw from, thus allowing for an improved understanding of their lived experiences (Alase, 2017). Eight participants were selected, all of whom have a similar professional experience, hence allowing for the capture of the commonality of their experience or phenomenon (Alase, 2017; Polkinghorne, 1989). To obtain a diverse range of experiences, a two by two matrix was developed using gender and years of experience as variables (see Figure 2).

Figure 2
Matrix of the Study Participants

Male Security Professionals ≤ 3 Years	Female Security Professionals ≥ 6 Years
Male Security Professionals ≥ 6 Years	Female Security Professionals ≤ 3 Years

The lower experience level is categorized as being at or below three years in a security role. The level of experience includes the accumulated time in any combination of security roles that may have been held regardless of security domain or industry. The upper level of experience is categorized as equal to or greater than six years of experience, and it includes the combined total

years of experience held regardless of the security role, the level of leadership in the organization, and the industry. The participants with more experience are expected to also have had more positions of authority or leadership, such as managers, directors, or higher, as well as more professional certifications that typically require a higher number of years of experience before being conferred. An example of one such certification requiring advanced knowledge of security and experience is the Certified Information Systems Security Professional (CISSP) certification, which obligates a holder to have a minimum of five years of experience in two different security domains before they can be awarded the certification. Participants with a few years of experience are expected to hold more individual contributor roles and have fewer professional certifications, as they have not yet met the requirements for more advanced security certifications. Women are an underrepresented group in the information security field; in fact, they constitute only 24% of the industry and continue to earn less than their male counterparts, according to *A Cybersecurity Workforce Report on Women in Cybersecurity* (isc2.org, 2020). Women in an information security role are expected to experience the tensions that their male counterparts would not experience as they engage in their roles. By selecting only those participants who are engaged in information security reporting, I used a literal replication to gather their similar experiences. Furthermore, by choosing different levels of experience and genders, I employed a theoretical replication to gather contradictory experiences between the two variables of experience and gender. This combination of literal and theoretical replications generated a sample of eight participants, each of whom was interviewed thrice times, thus creating 24 interviews.

All the participants were recruited from the Southwest region of the United States using recruitment emails sent from a professional association for information systems security professionals, of which the main researcher has a seat on the board of directors. In addition to

emails sent by the professional association, recruitment emails were also distributed to a list of contacts generated by the main researcher through years of experience in the information security field. The participants were not made aware of the researcher's role in the association's board of directors; nonetheless, this information may have been known to the participants through interaction with the association. The respondents were screened using a basic set of demographic questions to determine their eligibility for the study. The demographic questions included gender and years of experience in information security roles, which corresponded to the two variables mentioned earlier. Upon the determination of the participants' eligibility to take part in the study, they were asked about their ability to meet the interview schedule outlined in the interview protocol section. Those respondents who were neither willing nor able to commit to the interview protocol schedule were dropped from the list of study candidates. Upon the identification of the eligible participants, interview sessions were scheduled, and their interview sessions were initiated. This scheduling method was expected to create an overlap in interview sessions in which no particular group of participants was being interviewed at any one point during the interview. The study approach was selected for its theoretical replication, which seeks anticipated results related to all the participants' lived experiences related to their involvement in security reporting and the meaning they draw from the reflection on past and current experiences (Yin, 2018, p. 54). The number of participants was chosen for their homogeneity and ability to provide a rich and deeply analytical data set; additionally, such approach conforms to a phenomenological research tradition of using a participant pool size of less than 25 participants (Alase, 2017) while still allowing for a comparative analysis of the participants' experiences (Van de Ven, 2013). The combined total years of experience for all the participants was 46.5 years, with the lower level of experience averaging 2.63 years and the upper level of experience averaging nine years. The total combined

years of experience for males was 28.5 years, with the lower level of experience averaging 2.25 years and the upper level averaging 12 years of experience. The combined total years of experience for all the female participants was 12 years, with the lower level averaging three years and the upper level averaging six years of experience. The male: female ratio of experience was females accounting for 42.11% and males accounting for 57.89%. The average experience between male and female participants in the lower experience level was evenly distributed, with females accounting for 57.14% of the experience and males constituting the remaining 42.86%. In the upper levels of experience, the male participants accounted for 66.67% and females only 33.33% of the experience. This result was expected, as the percentage of female information security professionals in the field is currently 24%; this proportion has been growing over the years and as it increases, females are expected to boost their experience. Although education was not used as a variable for this study, 50% of the participants have a master's degree, 37.5% a bachelor's degree, and 12.5% a high school diploma. The participants have a large number of certifications; hence, unexpectedly, the average number of certifications held by participants between the two experience levels was fairly even, with the higher level of experience having on average 2.75 professional certifications each, whereas the participants with a lower level of experience held on average 2.0 professional certifications each.

III.2 Data Collection

Human experiences are transitory by nature and in need of reflection if people are to develop meaning from such experiences. A single interview would not provide participants with sufficient time to reflect on their experiences in meaningful ways. To overcome this limitation in reflection, we rely on Seidman's three-interview series (Seidman, 2013, p. 16).

Finding meaning in lived experiences is not a novel concept. Individuals are constantly finding meaning or significance in their lived experiences; however, drawing significance from these experiences is intuitive, and this process does not occur until people use language to deepen and transform these experiences that hitherto remain unexpanded and unrefined because they are stored as everyday occurrences (Merleau-Ponty & Landes, 2012). To reiterate, drawing meaning from experiences is intuitive, and this case is true whether in fiction or in real life. An example would be watching a movie of fiction in which a character loses a loved one or a pet. As the character experiences the anguish of the loss, the viewers begin to draw meaning from the character's experience. The viewers may possibly recall similarities to their own lived experiences and thus derive meaning from the very experience of watching the movie, which upon reflection can be analyzed and pondered. This reflection is the root of phenomenology, and interpretive phenomenological analysis seeks to understand the uniqueness of the meaning given to the experience upon reflection on the experience.

The purpose of this study seeks to understand the particular phenomenon experienced in the workplace by information security professionals from a paradoxical perspective and these experiences are not likely to stand out as monumental as say the birth of a child; thus, an approach was adopted to guide study participants in the reflection process. The approach was based on an in-depth interviewing methodology from the traditions of phenomenological research used to draw meaning from lived experiences (Alase, 2017). This is achieved by having participants draw meaning from interactions in their daily lives (van Manen, 2014). Increasing the understanding of the participants' behaviors and the meanings derived from their experiences entails their participation in a series of three interviews. Each interview was designed to reflect on the

experiences that the participant has had in dealing with information security reporting and the meanings developed from those experiences (Seidman, 2013, p. 14).

III.3 Interview Protocol

To facilitate the participants' active reflection on their lived experiences, each one was interviewed thrice. This approach was designed to allow the participants to reflect on the questions asked in each of the first two interview sessions, leading to the third interview in which the meanings of the experiences discussed in the first two interviews were uncovered. All the interview sessions were audio-recorded with the consent of each participant for transcription and coding during the analysis process. The audio recordings and any notes taken by the researcher during the session were used for generating specific questions tailored from the experiences described in the first two interview sessions for the final interview as a means of guiding the participants in the meaning-making process.

The initial interview was the basis for reflection, and it focused on the participants' past experiences and their roles prior to their current one. A semi-structured format was adopted for the interview questions. Moreover, several rules specific to each interview session were followed, such as an imposed time limit of 90 minutes, and those rules were emphasized during the recruitment phase and again at the beginning of each interview session. The average duration of the first interview across all eight participants was 57.75 minutes, with the longest interview lasting 75 minutes and the shortest interview lasting 24 minutes. Much of the participants' reflection was expected to transpire outside of the interview session, as they reflected on the interview questions and their responses during this interview session. During this initial interview, questions were asked that related only to the participants' previous roles or experiences to remind them of these instances that they might have faced in the workplace. These questions included "Tell me about a

time when you were asked to do something that went against company policy"; "Have you ever experienced a time when you felt that you had no good options? If so, what did you do?"; and "Were you ever asked to alter or manipulate a security report?". As the purpose of this study was to understand the tensions related to information security reporting, the interview questions were bracketed to this specific research topic area; however, the use of a semi-structured format was continued when the participants provided responses that strayed from the research topic. The participants were then allowed to give their answers, and a follow-up question was used to revert the discussion back to the topic. The goal in this case was to facilitate the participants' reflection on the general experience while guiding them to more specific details of their experiences related to the research topic. In this initial interview, the participants were asked to only provide facts of the experiences, such as the point at which these experiences transpired in their careers, the outcome of the event, and whether they still work with the same company or people involved in those experiences. The goal of this interview was to begin the recollection process, and no time was spent reflecting on the meanings of those experiences.

The second interview was conducted a minimum of two days following the initial interview but no more than seven days after the interview; on average, it was conducted four days after the initial interview. The lower time limit was set to provide the participants with the requisite time to reflect on the initial interview, whereas the upper time limit was established to reduce the likelihood that participants would begin to forget the reflections made between the interview sessions. Whenever possible, the first interview was not be discussed during the second interview to avoid straying into the meaning-making process that was reserved for the third interview session. Nevertheless, the participants were individually asked if they had thought of anything after the initial interview that they wish they had mentioned during the session. Only one

participant provided an experience they wished to have recorded. As with the initial interview, a strict 90-minute time limit was imposed, and similar fact-based questions were asked with the difference being that the participants were asked to reflect on experiences from their current role only. The average duration of the second interview was 42.88 minutes, with the longest session lasting 66 minutes and the shortest one lasting 29 minutes. The second interview session was on average approximately 15 minutes shorter in duration than the first one because the interview questions were limited to the participant's current role, whereas the initial interview covered all the previous roles. As with the initial interview, a semi-structured interview format was used and several questions were asked, such as "In your current role, have you had to deal with situations that contradicted themselves? If so, what did you do?"; "Have you recently had to deal with issues in which you felt that no good options were available?"; and "Have you been asked to alter or manipulate a security report?". The participants were once again asked to provide only the facts related to their experiences and to avoid any meaning making or emotions that could be generated as a result of recalling those experiences.

The third and final interview was conducted a minimum of two days but not more than seven days following the second interview, and it averaged five days after the second interview. This delay provided the researcher with time to create the questions for the third interview sessions based on the responses that the participants provided in the previous two interview sessions; the questions were designed to direct the participants in the reflection on those experiences and the meanings they gave to those reflections (van Manan, 2016). As with the first two interviews, a strict 90-minute time limit was imposed; however, in contrast to the first two interviews in which fact-based questions were asked, the participants in the third interview were asked to reflect on the experiences from the first two interviews. As a result, this final interview session had the longest

duration averaging 65 minutes, with the longest session lasting 82 minutes and the shortest one lasting 36 minutes. Special attention was given here to avoid too close a direction in guidance to prevent any loss of richness of the raw material while all questions were still bracketed to provide adequate direction for a meaningful guide in the reflection process (Walsham, 1995).

The participants were individually provided with a unique identifier to protect their identity, and these unique identifiers were used in all the interview notes and subsequent analysis. All the interview sessions were held in individual closed sessions that allowed the participants to speak freely and to avoid noise during the recording of the sessions. As soon as possible following each interview session, the digital recordings were transcribed using NVivo's transcription service. Once transcribed, all the transcriptions and any notes made by the researchers were then uploaded to NVivo 12 for analysis. Twenty-two hours of interview sessions were audio-recorded, and 819 pages of transcription data were generated.

III.4 Phenomenological Analysis

Phenomenological analysis is an interpretive process that requires the researcher to interpret the meanings of the study participants' lived experiences (Alase, 2017; Smith et al., 2013). Following the framework in Clark Moustakas' 1994 book *Phenomenological Research Methods*, the process of transcendental phenomenological analysis involves four stages. The first stage, epoché, involves the researcher's personal reflection as a means of recognizing that the researcher must consider what they already know and how it may color the analysis of the study data. This stage was especially important to this study, given that the main researcher is embedded in the information security field and has some experience with information security reports being altered or manipulated. In the second stage, phenomenological reduction, the coding and grouping of core meanings by the participants are initiated. The third stage of imaginative variation requires

the researcher to examine the possible meanings and interpretations of the themes generated in the previous stage. Finally, in the fourth stage of synthesis of meanings, the researcher develops the meanings of the participants' experiences. In this study, this four-stage process allowed the researcher to conduct multiple levels of analysis and to draw deep meaning from the experiences as the analysis moves through the abstraction from the whole to the individual themes. Each stage is discussed in detail in the subsequent sections.

III.4.1 Epoché

The first stage involves a personal reflection by the researcher. Developed by the founder of phenomenology, Edmund Husserl, epoché means to abstain or stay away from, and for the researcher, epoché means to avoid prior knowledge that may create biases, prejudices, and preconceived notions (Moustakas, 1994, p. 83). Hence, a focus on clearing the slate, starting with a fresh canvas where all ideas are viewed, understandings, and new awareness are considered evenly and with equal measure. Having prior experience with this research topic, the researcher repeatedly returned to this stage during the analysis and between each phase to ensure his own experiences were not generating a bias in the results. The outcome of the epoché should be that nothing is predetermined because we, as the researchers, have removed our preconceived biases, judgements, and determinations of what we were expecting. This stage inherently required a high level of awareness of presumptions that lead us to the study in the first place, and it serves to remind us that we must set aside those presumptions. Although the empirical analyses may indicate that prior beliefs and intuits held true, these factors were identified prior to taking any further steps by listing any presumptions of what the data may state before proceeding (Moustakas, 1994). Nonetheless, this avoidance of prior knowledge does not signify that all presumptions were

incorrect or excluded from the results, but rather that they did not have an effect on the final analysis by coloring the evaluation and interpretation process.

Epoché is not a one-time process but is an overall state of mind that by returning to as the study is conducted ensures that new ideas, concepts, and meanings were open to acceptance; furthermore, the repeated use of the epoché allowed to more easily remove myself from the data and to become attuned to what the data were conveying (Moustakas, 1994). As themes began to emerge later in the analysis, returning to the epoché was essential to ensure that new biases and beliefs have not closed my mind to fresh insights as a novel understanding of the phenomenon under study was developed.

III.4.2 Phenomenological Reduction

With an improved understanding of the inherent biases that are brought to the study, insights began to be drawn from the core meanings that the participants had developed by reflecting on their own experiences and how those experiences had added meaning to their lives (Smith, Flowers, & Larkin, 2013). Hence, key elements of the data were emphasized. First, the research was bracketed whereby all the other topics and questions were discarded, allowing the focus to be rooted on the research topic (Moustakas, 1994, p. 96). Moustakas uses the term "horizonalizing" and describes it as the act of taking all the statements as being equal (Moustakas, 1994, p. 97). By "horizonalizing," Moustakas indicates that all the statements made by the participants are given an equal weight, and no judgements are made at this stage of the analysis and nothing is categorized or counted as a duplicate. The participants' statements were individually reduced to their essences or themes. In a sense, the statements were paraphrased while retaining the purity of their substance and dismissing any scientific reference; additionally, statements that were unrelated to the research topic were removed, leaving only the meaning given by the

participant. As a result of this "horizonalizing," 283 tensions were detected as having been experienced across all the participants, and 119 instances of resolution actions to those tensions were identified. Themes began to emerge at this point; however, the researcher remained aware that each statement was equal to all the other statements, and duplicates were not removed despite the occurrence of clear patterns. Once all the statements had been reduced to their essence or theme, the analysis process began. Duplicate statements were now removed, and similar experiences were combined as they started to take shape as emergent themes (Miles, Huberman, & Saldana, 2014, p. 86); furthermore, at this point the relationships began to emerge between them as the gestalt of the phenomenon (Smith, Flowers, & Larkin, 2013, p. 79).

III.4.3 Imaginative Variation

The analysis began to draw insights from the emergent themes developed in the previous stage and started categorizing them into the possible meanings and essential structures of the phenomenon (Moustakas, 1994, p. 97). All the possible variations were examined and the different perspectives, roles, and interpretations were considered. In addition, the analysis began to consider causation, context, and relationships as potential variables for the structures that had emerged (Moustakas, 1994, p. 98). At this point in the analysis phase, the focus had been on the general collection of data, followed by a slow filtering of the data into themes, and finally the analysis of the data, viewing them from all angles and through different lenses. Questions were asked and detailed notes were taken as the transcripts of the interviews were repeatedly read line-by-line, with each reading taking a more critical view. In his 2018 book *Crafting Phenomenological Research*, Mark Vagle states that multiple, line-by-line reading passes should be taken, each with a different set of goals in mind, and all the transcripts should be read line-by-line before beginning a second line-by-line pass (Vagle, 2018, p. 110). In this first reading, detailed notes were taken

and comments were placed in the margin, along with parentheses or highlights for meanings that were clear. Later readings included the articulation of observations and concepts that began to appear. Vagle suggests at least three line-by-line readings of the transcripts to allow the repetition to lead to a careful examination and triangulation of themes (Vagle, 2018, p. 108). Four rounds of line-by-line readings were conducted, filtering down on each reading. At the end of this process, 118 unique experiences demonstrating tensions had been determined and 69 resolution actions to these tensions were identified across all participants.

III.4.4 Synthesis of Meanings and Essences

This final stage constitutes the core of the phenomenological analysis process and involves the meanings or essences of the participants' perceptions as they understand them (Merleau-Ponty & Landes 2012). The participants have their own perspectives of the world; hence, the researcher must find the essence of their experiences (Giorgi, 2017) by synthesizing the meanings and essences to uncover the gestalt of the phenomenon.

The synthesis represents the essences at the point in time for the participants and from each participant's unique standpoints, which do not signify an exhaustive study (Moustakas, 1994, p. 100). However, these unique viewpoints provide us with a representation of the phenomenon from the perspective of the participants for whom all have differing levels of experience in the research area. The outcome of this final stage of the analysis is an understanding of what was experienced and how it was experienced, which is the contextual nature of the experience and the phenomenological structure or meaning that was developed from the experience. This phenomenological structure separates the phenomenon from a researcher's personal interpretation (Jackson et al., 2018). The final synthesis resulted in the identification of seven paradoxical

tensions that affect the security reporting of information security professionals and the seven actions that they undertake in attempting to resolve these tensions.

CHAPTER IV. **RESULTS**

An information security professional is obliged to uphold the organization's information security policies, federal regulations, and industry standards. All professional information security certifications require the holder to uphold ethical/conduct standards. An example is the International Information Systems Security Certification Consortium $(ISC)^2$, which is recognized as one of the leaders in information security certifications requiring certification holders to agree to their code of ethics, including the adherence to "the highest ethical standards of behavior" (isc2.org, 2020). In this light, information security professionals are expected to act in an ethical manner. Even the ones who do not hold a professional certification are expected to act ethically in their role as a protector of an organization's assets. However, a thorough analysis of all the participants' experiences indicates that information security professionals are often confronted with unethical demands or practices that create a paradox (Lewis, 2000). These paradoxes are in the form of contradictions or mixed messages (Lewis, 2000; Putnam, 1986), and we have identified seven common drivers of tensions experienced by the participants, which resulted in the unethical behavior of false reporting or manipulation of information security reports. These seven drivers of tensions are unethical security culture, a fear of looking bad, tight deadlines or scoping issues, lack of experience or knowledge, perceptions of security, team politics, and coercion. In dealing with these drivers of tensions, information security professionals undertake actions to resolve the tension that often creates new tensions that must be addressed. Being forced to deal with a latent tension that brings the tension into salience frequently generates a paradox that must be managed. Based on the study results, seven common resolutions used by information security professionals to resolve the drivers of tensions emerged, including denying responsibility, attempting to change the organization, self-protection, self-education, repressing the tension, forming tight subgroups,

and withdrawing from the tension. The descriptions and respective examples as experienced by the participants are provided below.

IV.1 Drivers of Tensions

IV.1.1 Unethical Security Culture

Similar to individuals, organizations intend to portray themselves in the best possible light to outside observers. When information security professionals apply to an organization, they are presented with this portrait of virtue, and they cannot determine the true culture of the organization until they are able to see behind the curtain. One participant described his organization as a "paper fort" and stated,

> *It was a couple months in…[some of my co-workers and I] ended up referring to [the company] as a paper fort. It was like this image of grandeur in the security posture, [and] there was a lot of posturing.*

Culture in an organization is developed by management, and the demands that management make on security professionals reflect that culture. Many participants mentioned demands that met ethical standards, such as reducing a security finding because a mitigating control was in place that reduced the likelihood of the issue being exploited. However, they also identified many instances of unethical demands made by management.

One participant who was new to the industry described an instance in which he was involved in a security audit and the auditor asked for the screenshots of a four-month period for a certain system. The security professional was instructed by his management to gather the screenshots of a different period that looked better and to remove the date and time from the screenshot when providing the evidence to the auditor so the auditor would not know. When asked to further explain this incident, the participant stated,

> *When I was asked to do it, it was unusual. It seemed like an unusual request because when I was at [another company], that was the standard, you always collected the date and time; prior to that [situation]…my experience was nonexistent…I did not necessarily question it more than I reaffirmed their request with them to make sure that it was okay.*

When the participant later asked management why he was being advised to alter the evidence for a security audit report, he was advised to "not worry about it" and informed that the issue would be brushed off by management. As this example illustrates, management in an unethical security culture takes advantage of inexperienced security professionals.

Another participant recounted that early in her career, she was hired with neither any experience nor certifications and was instructed to perform tasks that violated industry regulations; furthermore, the organization would often joke about how inexperienced the new hires were and did not know any better. Once she achieved her professional certification, she realized the number of regulations being violated by the company:

> *I did not really understand the full ram of the standard..., once I actually went through that entire process [of] getting my certification and really, truly understanding…how my approach to this from an ethical perspective and from an interpretation perspective was correct. [Moreover], I have been told the wrong things all the time. That was [the moment] when I realized that, okay, Houston, we have a problem here.*

After realizing that management had been advising her incorrectly regarding the industry standards, she approached management with her concerns, only to be told that she simply did not know what she was talking about because she was relatively new to the industry. This type of statement was indicated by most participants from early in their careers when they asked management about practices that they felt were unethical or manipulative. Such unethical security culture becomes pervasive and information security professionals subsequently begin to accept it as the standard. As one participant noted,

> *There [were] no ethics. It was unethical around here that we all might as well just have some fun in the meantime. That's literally the attitude that a number of us adopted.*

This unethical culture is adopted by security professionals as management continues to make unethical or manipulative demands. These demands are most often made because of management's fears.

IV.1.2 Fear of Looking Bad

Management is the responsible party for information security reports that are delivered to the executive leadership. These reports frequently include information about areas where the organization is failing. Many participants described the management's fear of reporting unpleasant news to the executive leadership. As an example of this case, one participant who had a decade of experience in information security and had moved into a management role himself described why the reports were being altered:

> *Up the management chain is where things tend to get a little bit shifted in how they get reported…Matters are [frequently] downplayed just to save face…[hence], numerous risks become*

slightly muddled to make them look not as bad as they actually are

so that people don't look bad.

An experienced participant, a security analyst at the time, described a manager who was afraid to report security issues to the executives. This fear prompted him to alter all the reports they had generated. In one instance, an external team was hired to provide the organization with a baseline of the identity and access management (IAM) program. The goal was to obtain a real picture of where the program was currently so that efforts could be undertaken to mature the program. When the report was provided to the manager, he decided to alter it even before sending it to the board of directors. The manager justified this action by stating, "If this [report] gets to the board in this format, I'll be fired." The security analyst notified the HR department about the manager's actions; someone from HR proceeded to speak with the manager, but nothing was done and no reprimand was given. The security analyst later learned that the manager's senior leader was also altering the reports before they were sent to the executive leadership. As a result of this unethical security practice, the security team knew that two levels of management above them were altering the security reports and feared that if the issue were taken any higher, then the entire team would be fired.

Another participant was new to the security field after having changed careers from the financial industry. Having moved across the country to start a new career, the participant began work with a security team responsible for identifying and patching security vulnerabilities in the organization's network. He immediately realized that management did not care about the work that was being done and that only the final numbers were reported. The participant explained that when he first started, management did not seem to understand how the patching process worked. The organization had not patched any of its systems for several years, which indicated that the

patching process must be conducted in a layered approach, and a patch would often break other processes once applied. This highly manual process required an ample amount of time to complete. A patch that caused another issue would subsequently increase the number of total issues that were reported each week. The participant recalled a conversation with the manager, which demonstrated the latter's goals:

> *What can we do to fix this [issue]? I have to report it to the higher up. What can you do to the numbers to help me with this?*

The participant believed that his being new to the field was getting his team in trouble and the numbers being reported were his fault. He spent several months learning everything that he could about the process until he was certain that he was not the problem. To assist his team in getting the numbers where management wanted them, he would work off the clock on weekends and in the evenings to help lower the numbers for the weekly report. He approached the manager and tried to explain the nature of the problem and how the patching process worked. However, after repeated attempts to educate the manager on how the patching process worked and the manager continuing to insist on the total numbers being the only concern that mattered, the team lead began to alter the reports to please the manager. As the participant described,

> *Instead of reporting on the 35 systems that we manage, [we] only report on 10 of those and…make sure that they are the ones that the vulnerabilities are going down the most on.*

This case demonstrates how leadership sets the culture for the organization. As the security teams notice management acting in an unethical manner and making unethical demands on the security professionals, they begin to undertake the necessary actions to complete the job.

Another participant who was highly experienced at the time of the study described the unethical culture in a previous organization from early in her career:

> *[I was] in a company that…I really didn't care about. We would take three-hour lunches because…there [were] no ethics. It's unethical around here, [so] we all might as well have fun in the meantime.*

Reporting the unethical issues to leadership or to a regulatory body also generates fear for security professionals. As illustrated in the aforementioned example, reporting the issue to HR did nothing, and knowing that at least two levels of management above the team were altering reports produced the fear of being terminated.

Another participant who had several years of management experience was asked about reporting the unethical practices to a regulatory body. He replied that the reporting of any issues to the federal regulators would be a "sealed death wish," denoting that he was guaranteed to be terminated because the organization would know that he had reported the issues. As an example, the participant recounted an incident when a negative review was added to a job board. Within a few days of the review being posted, he was called into the office and "accused of making inflammatory, scandalous remarks against the company, without [being] given the option to defend [himself]." As the organization did not believe that he had not written the review, he decided to investigate the issue himself to save his job. The experience left him with no doubt that reporting issues to the federal regulators would result in the organization knowing where the report came from, stating, "If I were to make a complaint to a regulatory agency, they would know that it came from me." Several participants described similar experiences in which they attempted to report unethical behavior to leadership or to HR, only to realize that reporting did nothing to solve the

issue. Other participants underscored the fear of reporting unethical practices, indicating that the culture was such that unethical practices were the norm and reporting would result in their termination.

Some participants reported a fear of the manager and described demanding bosses, portraying behaviors that affected the reports as they attempted to avoid their supervisors. One participant explained that her manager was highly demanding and would question her endlessly about any security finding she reported. This level of scrutiny prompted her to alter how she would generate reports, stating,

> *When you're communicating to your manager and…intentionally avoiding digging in and just saying it's low risk to avoid that confrontation with your boss.*

Most of the issues reported by the participants were related to security roles that were internal to the organization. Nonetheless, external roles were not exempt from reporting issues related to fear.

Several participants held external information security roles at previous organizations, with four participants working in an external role at the time of the study. Similar to the internal roles, the security professionals who conducted external security reports also experienced levels of fear that affected the security reports; however, those fears were generally related to a fear of losing the client's business. One participant described an instance in which the organization had suffered a security breach. At the time, the participant was a new security manager with the organization and asked about the reporting process so as to properly notify the clients about the breach. The upper management team explicitly declared that no report would be given:

> *Absolutely not. We don't want [to] look bad. We already had some issues. We've been in the news…we can't allow this [situation] to*

> *be known because [the client] is just going to go over to [the competition].*

The upper management was afraid of losing their clients to the competition and because they had recently received some bad publicity, they refused to generate a breach report. Other participants described the management's fear of losing the business if the security reports had too many findings and not being invited back to conduct the security reviews in the future.

One participant who is new to the security field described the instructions that had been given by her manager in an attempt to ensure that the organization was asked to return in the future:

> *There was a bit more focus on…very careful word choice to still be accurate, but also not cause those feelings of, oh, we're not going to hire them in the future, because that's…part of doing [the] work, wanting to maintain a good reporting relationship.*

Although the preceding case was not described by many participants as unethical, some of them explained that management demanded that the wording be altered to reduce the impact of the findings on the security report. This attempt to reduce the impact of a finding on the security report to make the report appear less of an issue is not considered ethical. The report should be created using the facts to allow the organization's leadership to make decision how to resolve any issues the report has identified.

Moreover, all the participants mentioned issues that related to security reporting in one form or another, which were due to management's involvement in altering or ordering the modification of a security report or a fear of the manager that led to the security report being changed as a means of avoiding the manager.

IV.1.3 Tight Deadlines or Scoping Issues

Many participants reported that tight deadlines and scoping issues resulted in the security reports either being altered or lacking in accuracy due to the tensions they faced. Most of these examples were related to external security reporting roles and the time they were given to identify and report the security issues. Several examples that one participant provided included security engagements that were scoped for 40 hours of work. This time included detecting any security issues, validating those issues, and generating a report. Prior to the engagement being scoped for 40 hours, the number of security issues that would be found was unknown. In many instances, far more security issues were expected and could be validated in the time allotted for the engagement. In one case, the participant described that she would ask for more time to conduct the assessment. She would sometimes get more time and at other times she would not. In one instance of not being given sufficient time, she had a discussion with her manager:

> *If I'm neither generating a good report nor doing a deep-dive manual review, [then] do not blame me because you're not going to give me more than 40 hours.*

The participant described other members of her team who would only report on what they could in the time given and would ignore the rest. This approach would leave the security reports inaccurate, and many findings would not be reported. In many instances, the participants reported working extra hours off the clock to meet tight deadlines as a result of poor scoping prior to the engagement. When asked how this affected her life, the participant replied,

> *It's just very exhausting because you're putting in more hours, which again takes away time from your personal life…. It even*

impacts your health because you don't have enough time to do things that are beyond sitting at your desk.

One participant was advised by his doctor that for health reasons, he needed to leave the external security role he had been in for 10 years because of its negative impact on his health. The extra hours required to meet these deadlines affected not only the participant's health but also the security reporting.

Another participant who was working as an external security auditor explained that in addition to gaining weight due to the long hours she was working to meet the deadlines, she was putting in 65–70 hours, seven days a week because the company was assigning her 20 clients at a time. These long hours each week caused the reports to be rushed and some matters to be overlooked. According to the participant, her organization's requirement was to get as many security assessments completed as possible regardless of accuracy:

[We] pushed the clients through, regardless of their actual state, [and we were tasked to] handle 20 clients when we shouldn't. [Thus,] some things will be missed, which occurred all the time.

In this instance, the regulating body suggested each security assessor should not maintain more than three clients. Nonetheless, her organization would routinely have each assessor engaging with 20 clients at a time to drive the business growth.

In several instances the participants described issues with reporting due to limitations in the scope of the engagement. One participant recalled an engagement that had been scoped several years prior and was limited to only two types of security vulnerabilities she was allowed to report. When the participant would scan the applications for security vulnerabilities, she would find many different types of security issues; however, she was prevented from reporting them to the

organization because the scope of the engagement specified only two types of security vulnerabilities. Based on this limited scope, management refused to include any security vulnerabilities that were found in addition to the two that were mentioned in the scope of work.

Many participants described internal teams attempting to bypass the security team or to bring in the security team late into a project as they are close to the deadline, attempting to force the security team to provide a quick approval. One experienced participant, whose role as a security manager was to conduct phishing campaigns and report the results to show the number of people in the organization who fall for the fake phishing emails, underscored the executive management's attempts to falsely increase the pass rate. The executive would require the manager to notify him prior to sending out the phishing campaign; the executive would subsequently alert the organization about the phishing emails that were coming and alert everyone to be ready for them. To contend with this executive's attempt to manipulate the data, the security manager had to alter his approach:

> *I just…resolved it myself and just [did] it all in one shot instead of over a two or three-week period. I still told them I was doing it, I just sent it all out in one shot to get a…more accurate number.*

All the participants mentioned some form of deadline or scoping issue that influenced the security reports. Most of them acknowledged working extra hours on their own time to meet the deadlines, with many stating that poorly scoped security engagements had the largest effect on the reports due to time constraints. Those time constraints were usually due to a higher than expected number of security findings, whereas others were due to the security teams being brought in late in an attempt to reduce the amount of time within which to perform their reporting function.

IV.1.4 Lack of Experience or Knowledge

For the participants, the lack of experience or knowledge was related to both management and the security professionals being managed. However, this lack of experience was not limited to those working in the security field but was extended to those security professionals engaged in their reporting roles. For security professionals, this lack of experience was typically related to being new to the field or when changing to a new security domain. One participant recounted a case in which new security analysts were writing reports after validating their findings:

> *That expertise wasn't there…yet to ensure if it's being vetted correctly or not; a couple of analysts would not report everything, and it turned out that they were missing out [on] true positive findings.*

Another participant who at the time was a manager described a similar issue they experienced in their own team from new security analysts whom they supervised. The team was responsible for triaging security issues that were sent to them through a ticketing system. The analysts would quickly close out a security ticket, and the participant began questioning whether the issue was actually resolved:

> *A lot of times you would actually question the amount of visibility that the team had [or] how well they can actually deep dive into an issue. So, you would [repeatedly] see an issue get closed pretty quickly and you'd scratch your head a little bit and say, okay, is that…really addressed, or are we just moving right along because we're a little bit blind*

With new security managers, the lack of experience was portrayed as typically resulting in a lack of confidence that leads to security reports being submitted in an automated fashion instead of having the findings vetted for fear of the team missing a false positive.

A more experienced female participant stated that she disagreed with her team supervisor on what should be included in the security report. She argued that false positives should be removed to make the security report as accurate as possible and to avoid the false positives causing confusion in the final report. As she explained, "Initially, the person…whom I was reporting to was not as experienced." This lack of experience prompted the supervisor to require the team to report everything to the client because she was not adequately experienced to be confident that all the false positives were being properly vetted before being removed from the report. The same participant later indicated that a new, more experienced supervisor came in, and the team began vetting the findings and generating more accurate security reports.

Another experienced female participant was hired as a security manager for an organization. During the interview sessions, she was advised that her department would be audited in two months after she started; just two weeks into her new role, the participant received an email from the security auditor advising her that he would be there the next day. In this instance, the participant described going into the security audit completely unprepared and with very limited knowledge of the organization on which she was being audited. During the security audit, she was joined by her chief information security officer (CISO) who was also not knowledgeable in the areas being audited. As the participant recalled,

> *We were noncompliant in so many areas; I was two weeks [in], and I didn't know who to go to. [Even] my CISO [claimed that] he didn't*

know who to go to[stating]…the manager who was here before you did all that.

The participant described answering to the best of her ability with the limited knowledge she had and not directly answering other questions, with the CISO seated behind the assessor shaking his head yes or no depending on the question. Although this situation was not directly related to the altering of security reports, it demonstrated the types of inexperience that the security professionals must deal with, which affect the accuracy of the reports.

Similar to the previous situation, several participants mentioned working with stakeholders to gather the information they needed to generate the security reports. When asked if the stakeholders ever provided false information, an inexperienced female participant advised that such cases frequently occurred yet proved difficult to catch:

You can tell when they don't give you the [entire] story; instead they just offer a small piece of the pie and try to evade.

When asked to provide an example of this evasion, the participant cited a client who was queried about a very specific encryption setting:

I remember [an incident when] we, as an audit team, became convinced that it was not [encrypted], and they were not showing us and not really understanding…[that] we needed to see a specific functionality; it's a screen that's a check box [indicating whether] it's encrypted or not. They sort of avoided showing us that screen.

Many of the participants described similar issues and confirmed the difficulty in catching the stakeholders providing false information. This evasion and false information have a direct effect

on the accuracy of security reports. The participants repeatedly depicted these stakeholders' actions as being due to a perception of the security teams, which leads them to fear security.

IV.1.5 Perceptions of Security

As mentioned in the previous section, security professionals must deal with stakeholders to gather the information needed to generate security reports. This effort is often hampered by the perception that many stakeholders have of information security teams. Many stakeholders are afraid to engage the security teams. One participant with over a decade of experience in information security described how many stakeholders he has encountered over the years feel about security stating:

> *The main issue that I've seen over and over and over again in companies is that IT is trying to move at 60 mph, [striving] to meet the demands of the business, and [then] security comes along. I don't know that security necessarily says, [you] need to be going at 45 mph, but I think that that's the perception that IT gets from security, [suggesting the] need to slow down in what you're doing, making sure you're thinking through it, but that doesn't necessarily lead to the best practices.*

This perception of security engenders many of the issues that security professionals experience, which affect the security report when working with stakeholders.

Another participant new to his career described working with a high-level manager who would bypass the security teams altogether because her experience was that security was going to prevent her from doing what she felt was necessary. As soon as an issue was sent for review by

the security team, she would escalate the issue to the executive team in an attempt to remove the security teams from the decision process.

A participant who now owns his own security consulting business explained that this perception of security is due to the security teams and the IT department all reporting to the chief information officer (CIO). As he explained,

> *The outcomes and the objectives, what they're measured on, are vastly different. So, IT gets beaten up by the business to deliver solutions in enablement as quickly as possible, whereas security is sometimes perceived as a roadblock to both of those [efforts].*

Two teams that closely work together are the application development teams and the application security teams. The application security team is responsible for scanning the applications for security vulnerabilities prior to the usage of the application in a production environment. This aspect causes the development team's general dislike for the security team. In describing this rivalry, an experienced participant noted that the application development team felt that the application security team was similar to "somebody who passes on numerous commands and [acts in an]…extremely authoritative manner, [which] somewhat also creates a gap between the app teams and the security teams." The participants concurred that this rivalry has led to many instances in which the application teams would delay the submission of information to the security team to prevent the latter from reporting issues, or constantly insist that the security team was wrong and continuously demand that the security team proves its findings in an attempt to wear down the team.

Most of the experiences that the participants provided were related to internal stakeholders or departments and their perceptions of the security teams. One experienced participant expressed his perspective on security teams:

> *As [an external] consultant, [I notice that] you are insulated from the internal politics and the internal battles that occur. You could see [the situation] happening. The writing was on the wall, but I would say most of the time you're out of the room when those kinds of conversations happen.*

Although external security professionals are not as directly affected as the internal teams, they are also influenced by the perceptions of the security teams.

In addition to this perception, external security professionals had to deal with the client's certain level of mistrust. An experienced participant described her experience with this distrust as follows:

> *[The clients] already have some perception that they're not sure whether the work is quality work or not, or…who exactly has worked on it. They do not know much about the person, So, I think the doubts kind of… build…and [this mindset] reflects [in their behavior].*

With regard to offshore security teams, the perceptions are even more pronounced. The same participant, who had several years of experience in an offshore security team, recalled one such instance:

> *Clients expect that the consultant does everything because they are paying us for the work. So, we are answerable for everything. In that case, we are doing the assessment and helping them to build out a*

program…everything is expected. [However,] it's not possible to get everything done within 40 hours a week.

This perception that members of the security team are responsible for everything because they are being paid to perform a job results in a huge demand on the offshore consultants assigned to the client. As previously mentioned, when the scope of the engagement does not allow sufficient time for completion within 40 hours, the ensuing reports become inaccurate; unless the security professional works off the clock to meet the demands, many issues do not get reported.

Not every experience that the participants described was a negative one. A participant cited an instance in which an internal department head asked the security team to alter a security report to make it appear as a higher risk than the security team was reporting it. As the department head perceived the security team as being capable of advancing his initiatives, he used the altered report to gain a budget that he felt was needed to move the initiative forward.

IV.1.6 Team Politics

Most teams have some level of politics that are inherent and build over time as the individuals work with each other. This case is also true for information security teams; nonetheless, most of the participants stated these team politics as being responsible in many instances for inaccuracies in the security reports. A participant who had close to three years of experience at the time cited an occurrence in which a security analyst was holding a grudge against a manager and would bypass the QA process and instead directly send the security report to the client. The intent was to get the manager in trouble for any mistakes in the report. The same analyst stated that they would do anything they could to distort the quality of the work because they did not care about the work and wanted the manager to look bad. As the participant explained,

> *They didn't care about the work. [The situation] was more personal. I think they took [it] more personally. They didn't care…if they did not agree with the upper management or the lead; they would do whatever distorted it.*

The same participant recalled that upon assuming a new role, she was met by a man who had been with the organization for over a decade. She initially thought that he was attempting to help her and was interested in how she found and validated security vulnerabilities. She immediately realized that he was uninterested in learning from her but rather was attempting to sabotage her. This individual would ask her throughout the day about the matters she was working on. He would subsequently report to her supervisor that she was not doing what she was supposed to be doing according to him. When her manager spoke with her, he advised her that this individual had applied for the role she had but was denied. As a result, he was constantly trying to communicate with her each day and made the work environment hostile, causing her to dislike going to the office and bringing a negative effect to her security reporting.

An experienced participant described an experience with an application developer. When the participant started with a new organization, she made a mistake in scanning an application, which resulted in the scan going much deeper than expected. As a result, the application development team began to question everything that she had done and even suggested that she be terminated for the mistake. As she gained further experience and became more proficient, the dislike persisted, and the application development team would deny any finding she uncovered when scanning their application, thereby making her job more difficult. The participant described one encounter in which the application development team refused to accept her finding report and scheduled a meeting to demand that she explain herself. She described this encounter as follows:

> *He had his team involved in the call, and his leads, my leads, and I were all involved. I had to be on the call and he wanted me to speak up on the call instead of anybody else because…I guess it was just somebody who…already made a mistake, and this again was the same person. [However,] I did show him that [it] was a cross-site script.*

After proving her finding in front of the team supervisors for both teams, the issue did not improve between her and the individual from the development team, as the application development team did not want to look bad and its members felt embarrassed that she was able to find an exploit and prove it in front of everyone. This same participant described how office politics would impede in her obtaining the information she needed to complete the security reports. When she would ask for a particular training or documentation that she required to conduct a security review, she would be blocked by the individual responsible for approving it due to her relationship with someone this individual had a clash with inside the office. As a result, she could not perform her job properly, and the security report would suffer.

Several participants mentioned security analysts who would intentionally neglect their responsibilities so that others on the team would be forced to step in and perform the task they had avoided. An inexperienced participant recounted an issue at his first company where the team would designate one individual each day to work the "hot seat," that is, the ticketing queue. At the time, the individual was responsible for reviewing and remediating the security issues that were sent to the team while everyone else on the team would work on their individual assignments or special projects. As the participant explained,

> *People are assigned the hot seat daily; on certain days, you can see the tickets go down and on other days, the tickets really aren't getting picked up.*

This situation caused the rest of the team to pick up the extra work for those analysts who were not working the "hot seat" as required, resulting in less time for the security analysts to work on their security reports.

Another participant cited a similar experience early in his career, in which the organization had certain service level agreements to resolve high-priority tickets within 15 minutes of opening them. As some security issues were more difficult to resolve than others, several security analysts would only open the lower priority tickets that were easier to resolve within the 15-minute requirement. As a result, the high-level security issues would sit in the queue for sometimes six to eight hours before someone would begin working on them. From a security perspective, this delay had the potential to allow an attacker in the network for that many hours before the issue was even reviewed.

IV.1.7 Coercion

The participants often mentioned discussions with their supervisors and leadership team addressing the unethical demands they were being given. Several participants stated their refusal to sign off on altered or manipulated reports; furthermore, in almost all of these encounters, the participants described their leadership's attempt at coercion when their demands were refused, and intimidation failed. Most attempts at coercion can be considered mild, but many participants indicated coercion attempts that went past the mild nature. The same common theme was observed in every example of extreme coercion that the participants depicted. It typically followed the same model whereby a threat was not directed at the individual but rather at those with whom they

worked. In addition, several participants acknowledged their refusal to act unethically and instead expressed a willingness to accept the consequences for their refusal. However, these same participants faltered when confronted with the consequences being paid by others in the organization.

Many instances that the participants described regarding security professionals interacting with stakeholders included mild forms of coercion attempt to convince them to alter the report or reduce a finding. As one inexperienced female participant who conducts security and privacy audits indicated, stakeholders would make statements as follows:

> *My boss is not going to like it if this issue or this finding comes up on my report, and [I'm] responsible for it.*

Other participants mentioned similar instances in which stakeholders would make statements asking if there was any way the security professional could help them with the report because they were afraid that their boss would fire them if they did not get it changed. A participant, who at the time was a security manager, recalled a case in which he refused to sign off on an altered report for ethical reasons. However, his leadership waited until he was out of the office and subsequently directed one of his subordinates to sign off, stating that "the security analysts were afraid to say 'no' to the upper management."

A female participant new to the security field described her experience in which a client tried to get the security analyst to reduce the severity of their findings, claiming the test was improperly conducted, or that the findings were false positives even though the findings had been validated. The intent was to scare the security analyst into changing the findings for fear of being made to look incompetent.

Several instances of more extreme coercion attempts were highlighted by the more experienced participants. One participant mentioned an experience from early in her career when the organization instructed her to do whatever it took to ensure that a major client passed the security assessment. To ensure that she did what she was told, the organization attempted to threaten her coworkers:

> *This is how we're going to pay our bonuses; this is how we're going to be able to close the year and hire more people.*

As the participant explained, the organization threatened them with the non-payment of Christmas bonuses if she did not comply with the directive. She added that her organization's attempt to threaten her into compliance with unethical demands was expressed as follows:

> *If we lose this client, then you're talking about losing jobs. People are going to lose their jobs. [Such statement] was literally [articulated] upfront. A lot of times, [the discussion] would go back to that statement, or [even this one]: "we're going to lose this big client to our competition up the street and…people are going to lose their jobs."*

The participant believed that "they [somehow] knew that this string was the one to pull with me and they pulled it, they pulled it very well."

Another participant who at the time was highly experienced in his career described an instance involving his organization where his leadership ordered him to ensure that a security report had a certain outcome:

> *I was told that if the outcome was X, then it would be bad for everyone. Therefore, the outcome should be Y. I was then told to figure out how to [turn] X into Y.*

When asked if he felt that the consequences would solely fall on him, he replied that he was told that "It would be bad for everyone."

A male participant with several years of management experience cited a case involving his organization, which escalated to coercion. He recalled that the leadership initially attempted to convince the security manager to sign off on a security report that included findings that had not been remediated. The reason was that the client had threatened to take its business elsewhere. The company was willing to sign off on the bad report because it did not intend to lose the client's money. The participant explained that the threats from upper management were initially subtle, beginning with a demand that he sign off on the report. The leadership became increasingly manipulative and used coercion (i.e., if he did not sign off, the company might fail, or people would be fired). Although the company never made a direct threat to him, it opted to threaten others in the organization.

IV.2 Resolution Actions

As previously mentioned, information security professionals are forced to deal with these drivers of tensions, and in doing so, those tensions become salient and must be addressed. In many instances, as the tension is resolved, it develops into an entirely new tension that must again be handled (Lewis, 2000; Putnam et al., 2016). Dealing with these salient tensions compels an individual to choose between two competing requirements; hence, these two competing requirements become a paradoxical tension. This study identifies seven common themes that the participants described based on their information security reporting-related experiences. The

resolution steps undertaken by the participants are viewed not through a moral lens that distinguishes right from wrong but rather from the demonstrated actions that the participants performed in resolving those tensions.

IV.2.1 Denying Responsibility

The main resolution step undertaken by the participants was to deny responsibility for any unethical behavior that they might have committed. Even when the participants acknowledged other resolution steps taken when confronted by a tension, most of them either started or ended with their lack of responsibility for the unethical behavior.

For a participant who was still new to the information security field (i.e., having less than three years of experience), this resolution step was primarily employed for contending with a paradoxical tension. He was able to cope with management's demands that he felt were unethical by putting the responsibility on management who had made the unethical demand. The participant provided several examples of this behavior and described one experience where he was involved in a security audit and the security auditor requested that the organization provide her with screenshots from a specific four-month period. The participant was instructed to alter the evidence before giving it to the security auditor by providing a different time period that looked better and making sure that the screenshots excluded the date and time so the auditor could not tell that the evidence was being fabricated. When asked about his role in this unethical behavior, the participant denied responsibility twice, once placing the responsibility on the auditor, noting, "I think it's up to the auditor to be able to attest that the date and time provided are accurate." He added that he did not excessively worry about providing the false evidence because he felt it was the auditor's responsibility to validate the evidence she was given, stating, "If it was a big deal, [then] the auditor

would say something." When pushed further on the subject, the participant placed the responsibility on the manager:

> *There was a little bit of a conflict when it came to providing the evidence that I was told to provide versus the evidence I believe I should have provided. Did I challenge that (issue)? No, I didn't. It was basically at the direction of my supervisor, and so I [simply complied] when they told me to provide the evidence [that they wanted].*

This experience was common with those participants early in their careers at the time of the study. In addition, the more experienced participants described similar experiences from early in their careers.

An experienced participant who described his earlier career explained that he was initially worried about getting caught altering the security reports, but he eventually decided that he was only doing what management had wanted. He knew that he was mentally justifying his actions by indicating that the responsibility was on management's shoulders and not his own, but he was also aware that should he be questioned, he would be unable to justify his actions.

For many of the participants, the primary reason for denying responsibility was their financial position at the time. These experiences were described by those participants in the lower experience group as more current and the ones in the more experience group as transpiring early in their careers. An inexperienced participant cited an experience where he had relocated from the East Coast to the West Coast at his own expense to begin his security career. He was not in a financial position to be able to walk away once he realized the unethical practices that were being required of him. As he stated,

> *Nobody was financially in a place where we could hold our ethics higher…So, it was okay if this is what they're asking for and I'm going to keep my job; I'm going to give them what they asked for.*

The participant added that he was afraid of not only losing his job because of his financial position but also of being caught engaging in the unethical behavior. He states that he was a combat vet and had seen combat including being blown up and shot at and was never as afraid as he was when thinking about being caught and losing his job.

The lack of a financial ability to walk away from a role was the most common reason given for continuing to perform unethical actions when management demanded them. All the participants described their attempts to speak out when they felt that the demand was unethical; nonetheless, even the most experienced participants would eventually relent and engage in the unethical action.

One participant new in her career explained that she tries to speak up and make her voice heard when she feels that something is not right, but management simply ignores her. Hence, she simply leaves the matter alone and justifies it as management's responsibility, even as she raises her objections.

Another female participant new in her career explained that at her level, she feels that if she were to be confronted by someone whom she believed was unethical, she would report it to her leader and the matter would then become the leadership's responsibility. If nothing is done, then the burden is not on her because she took action to report it.

IV.2.2 Attempting to Change the Organization

Once the participants realized that their organization has an unethical security culture or are asked to engage in an unethical action to alter a security report or manipulate evidence, they all described attempts to change the organization. As an experienced male participant explained,

> *It's that bit of an idealistic approach…I'm here to change this and make it better. And…it was articulated that there was support for this. [However,] after a period of time, it was just lip service…. I tried some different avenues and [even attempted] to escalate the various channels, but again, nothing happened.*

This participant was advised by the leadership at the time he was hired that he was being brought in to help mature the security culture and to search ways of improving the program, and he was promised full support from the leadership.

Another experienced male participant explained that when he first came to the organization, he strived to improve the security culture, but the leadership would fight him on everything. He eventually stopped trying to fight. The attempts to change an organization were generally described by the more experienced participants as they recounted their earlier career experiences.

An experienced female participant recalled that when she first started as an assessor in a highly regulated field, she had no experience and had to rely on her management to direct her in what should be done. Once she earned a professional certification and knew the regulatory requirements and industry standards, she realized that the company was conducting numerous activities that were in violation of the regulations. She initially tried to explain the areas where the organization was failing against the standards, but she was ignored and told that she was too new and did not know anything. This participant later refused to sign off on a report that lacked accurate information, believing that doing so would be unethical. Her organization simply had another of the senior assessors sign off on her work. Several attempts were eventually made, and she realized that regardless of her efforts, the organization would not change:

> *Okay, I am done, you're not even trying to fix anything. I understand we're all stressed, and I understand you have a small organization…we're screwing up clients' information. I [finally said to myself] that's it, I'm done.*

The more experienced participants mentioned similar experiences that ultimately led to their leaving the organization. The aforementioned participant stated that she knew that the company was unethical and had an unethical security culture, and she tried to fix it at first; she eventually realized that nothing she did was going to fix the organization.

An experienced male participant cited the same experience; after realizing that the company was unwilling to change and the senior leadership was unethical in altering the security reports, he began to mentally check out. He no longer had faith in the company and acknowledged that he could not work to make positive changes.

IV.2.3 Self-protection

As the participants began to realize that efforts to change the organization were not working and started to fear being associated with the unethical behavior being demanded of them by management, they described taking actions to protect themselves should their actions be noticed. The most common form of self-protection involved documenting the management's unethical demands. According to one experienced female participant, she began to record the issues that she believed were unethical. When management would instruct her to change a security report that did not comply with a regulation or industry standard, she would document what management had directed her to do. She resorted to this move to ensure that certain matters were recorded to show her disagreement with the practice.

In a similar case, an experienced male participant related how the upper management was altering the security reports before submitting them to the board of directors:

> *We definitely retained all of our copies of how [the materials] were drafted. Sometimes even during the revisions, we would change [issues] back to the state from which they were [altered].*

Retaining the original copies or adding notes to the original one was a common theme for many participants, and it became a practice that they continued to employ into their careers. As one of the less experienced female participants explained, in addition to her own notes and documentation, she would include comments in her assessments that she disagreed with the approach, but that management wanted it done in a certain manner. She said that she would exhaust all efforts that could serve as evidence that she was not acting unethically, but that management was.

In another example, an experienced male participant recounted that early in his career, his manager would generate two sets of reports. One report included a comprehensive set of numbers for all of the systems and a second one that was altered to remove the systems that had bad numbers as management requested. The second report was sent to the leadership, but the original security report was stored in the manager's desk drawer in case anything came back on the team.

A female participant who is early in her career revealed that she forces management to say or write out exactly what they want her to do when she perceives that the action to be unethical or against an industry regulation as a way of protecting herself. However, she would still express her dislike and provide them with an explanation of how it should be done, knowing that management would simply ignore her.

Another participant who is also early in her career explained a similar approach that she adopted:

> *The whole CYA thing, like the fact that I feel I need to do that for myself and my own job…so I can point the finger and say, "I didn't do this, and I didn't agree with this," if it were to come back to me.*

These similar experiences were described by all the participants and were developed very early in their careers. Many of the more experienced participants continue this practice into their present roles, although their current organizations do not have the same unethical security culture that they experienced early in their security career.

IV.2.4 Self-education

Many participants described actions to educate themselves when faced with a tension. For example, a participant who was early in his career as a security analyst revealed that management had demanded that his team reduce the number of security vulnerabilities in the organization's systems. The manager hardly cared about how diligently the team was working or how experienced the team members were but only expressed an interest in the fact that the total numbers were declining each week. The participant initially felt that his lack of experience was the reason for the failure and consequently made an effort to educate himself and become an asset to the team. He immediately realized that his abilities were not the reason for the failure; nevertheless, he continued to educate himself so that he could explain to the manager the cause of the failure in an attempt to discourage the manager from demanding the alteration of security reports to show his preferred yet fabricated numbers.

An experienced participant described the actions she had undertaken early in her career to self-educate after being denied access to training required to perform her job. She stated that when

she would neither get the help that she needed nor receive the requisite training, she resorted to obtaining the training on her own and educate herself to effectively perform her job. At the time, her role was to generate security reports, and being denied the necessary training affected her reporting ability.

Another experienced participant recounted how in her first security role she lacked experience in the security field and simply followed orders. As she began to self-study for an industry certification, she began to realize that her organization was making her perform tasks in a way that violated the industry standards and often regulatory requirements. This realization motivated her to learn as much and as quickly as she could.

> *I obtained my certification after four months [of self-study]. I was able to do so because that type of mentality that [the organization] had really pushed me to want to prove them wrong…especially [in terms of] interpreting the standard…more so than anything because they would say, "you don't know what we've been doing for years, so you don't really understand the interpretation." I worked really hard to understand and learn the ins and outs [of my job].*

The participant's awareness of her being instructed to perform unethically drove her to learn and to try and educate the organization on its failings. She later realized that she would be unable to change the organization but that she could be an example of how the job should be done correctly.

With regard to her first role, a participant in the lower experience group revealed that she realized beforehand that she did not want to remain in the role; nonetheless, she disliked the idea of letting her résumé "suffer" by changing out of her role too early. Instead she elected to stay for

a year and learn all she could to make herself more marketable for a future position at another organization.

IV.2.5 Repressing the Tension

Several participants acknowledged undertaking resolution actions to repress the tensions that they were forced to handle. This move typically occurred after one or more attempts to resolve the tension had failed or after a previous resolution action had created a new tension that they were then compelled to confront. In describing his time as a security manager, an experienced participant realized that his efforts to make changes in the organization had failed and he had lost the support of leadership. He had to adopt a "self-preservation" mode until he could find a new job.

> *I was an extravert when I was in the military. I was always out there in front, always leading, always involved. [However,] with this new position, the new job, the new attitude I have, I'm a complete introvert. I never leave my cubicle and I never talk to anybody unless spoken to first. I don't attend the social gatherings that the employer organizes. I don't socialize either. I just keep to myself and do my job; I keep my nose clean out of fear of what would happen should someone view my actions negatively.*

This experience demonstrated how the participant progressed toward the complete elimination of the chance of being forced to deal with any new tensions, as the refusal to speak to anyone unless forced to is repressing the current tensions.

An experienced participant recalled a similar incident from early in her career at a previous organization. She stated that she had to keep her paycheck coming in while she gained the

experience and learned the industry regulations. Although she was aware that the activities were being conducted incorrectly, she did what she had to until she found an opportunity to leave. In this example, the participant ignored the tension until she could find another role. She believed that she could disregard the issue and not have to deal with it long enough to make the tension go away.

Another experienced participant explained how she coped with the tension of being ignored by management early on when she would suggest the proper way of conducting activities:

> *I would reason it out…if I feel that a rationale exists or if [such activity constitutes a] policy, I cannot change policy. So, I agreed to what was being expected.*

She added that she would repress the tension by deciding to view any tension as most likely being a policy issue because she knew that she could not make policy changes.

IV.2.6 Forming Tight Subgroups

All the participants described working in teams at some point in their careers. Several participants mentioned the tensions that their entire team dealt with as the management made demands that were unethical and, in many instances, in violation of federal regulations. They also underscored how their teams had come together to form tight bonds as they coped with these demands. These bonds frequently engendered subgroups that divided themselves from the group, thus creating tension (i.e., a team of security analysts against the management). An experienced male participant recalled a case involving a team he was with early in his career:

> *We somewhat became friends because we went to lunch together on a regular basis. We dealt with the same problems. [These instances] somehow made [things] easier than I think they would have been.*

This collective experience allowed the participant to speak with his team members and share his frustrations over the management's demands. He mentioned battling the management as the team members would be forced to rely on each other to keep management off their backs. He also revealed how they convened informal meetings to decide the necessary steps in making the management happy. He added that several team members who held industry certifications worried about being caught altering reports at the behest of management and consequently losing their certifications. At these informal meetings, the team would discuss the steps they would take should they be found out.

Another experienced participant who was a security manager and leader of a team of security analysts at the time recounted a particular incident in which he worked to protect his subordinates from the upper management who wanted to blame his analysts for the security reports.

> *To me, it's more important that the subordinates don't get caught in the crossfire…so, I exert extra [efforts to] take care of them and protect them from the crossfire, although I do not need to.*

This type of protection did not go unnoticed by the security analysts. More than one participant mentioned the turnover of security analysts due to the conflict between the team and management or between their manager and upper management.

IV.2.7 Withdrawing from the Tension

All the participants eventually opted to withdraw from the tensions they faced, but not until after attempting one or more of the previously described resolution actions. The participants individually recounted their experiences whereby they knew that they could no longer remain at their organization and subsequently made plans to leave. Only one of the less experienced

participants, who did not describe the security culture as unethical, withdrew from the tensions that were not unscrupulous in nature. The remaining participants withdrew from tensions created by unethical demands and unethical security cultures. In most instances, the participants revealed that they stayed at their company for a year or more before leaving. However, one experienced female participant noted her decision to leave after only eight months with the organization following a major breach in the firm and the firm decided to cover it up.

> *I informed them all [about the breach]; the CEO [was] sitting in the same room. I asked, "What's the notification process?" I was the information security manager at the time and they replied, "Communicate? We're not communicating this."*

She mentioned the CEO's decision to hide the data breach and refusal to even notify the pertinent client for fear of losing that client. No matter the arguments that the participant had raised, the CEO refused to let her issue a breach notification. Realizing that she had no higher management to notify as the CEO had already made the decision, she decided that same day to leave and gave a 30-day notice.

Another experienced participant revealed that he could no longer endure management's unethical decisions. In a particular instance, he was ordered to remove the fact that an attacker had been in the network for four months and the organization had proof of this issue; however, to avoid penalties or fines, the organization decided to remove this information from the report to appear as though that it had been reported within the required timeframe. He referred to this incident as the last straw and eventually put in a two-week notice.

A more experienced male participant recalled his decision to leave after remaining with the organization for exactly two years.

> *I was the first one to leave. Within a period of six to eight months, everybody who was on the security operations side had left. Six to seven people on leadership positions had left.*

This participant was part of a leadership team that had formed a very tight subgroup as they defended themselves and their subordinates from the upper management's unethical demands; after the participant had left, almost the whole leadership team also quit the organization as the subgroup they had formed began to break up as individuals began leaving the organization.

For a less experienced female participant, she realized that she was altering her security reports in ways to avoid her overbearing manager and acknowledged that she was demotivated in her reporting work because of the manager's excessive demands. She then began looking for a different role at another organization.

Most of the participants described similar experiences in which they and others around them recognized their unethical security culture and their efforts to change the culture were failing. Upon realizing that they could not resolve the tensions, they decided to leave their current unethical security culture, desiring to engage with a better, ethical, organization.

CHAPTER V. **DISCUSSION**

Information security professionals are expected to act in an ethical manner and to report security issues to their organizations. Additionally, those with professional certifications have sworn to engage in ethical behaviors when accepting their certifications. These reports are expected to be complete and represent an accurate picture of an organization's needs, as the reports are used to strengthen the security posture against threats both internal and external to the organization. However, as this study indicates, these information security professionals must resolve many drivers of tensions and dealing with these tensions often creates a paradox. Security professionals must therefore decide between two opposing requirements, which often results in the security reports being altered or manipulated before being presented to the executive leadership. This situation also creates a paradox for the organization, that is, the firm must rely on the information security professional to generate the reports used to secure the organization, but the security reports are often altered or manipulated to reduce or hide the threats confronting the firm.

The participants described working at both small and large organizations. One experienced participant described being employed as a security manager at a small organization that employed 25 or fewer people, including the CEO. In this role, she directly interacted with the CEO who engaged in and ordered the participant to undertake unethical behaviors. The majority of participants reported working in large organizations, with several organizations employing 10,000 or more employees. The participants employed at larger organizations cited the unethical demands being made by leadership that was one or two levels above them, with a few participants reporting unethical demands coming from three levels of leadership above them. In the experiences described by the participants who were employed at larger organizations, none involved the unethical demands originating from the executive leadership (i.e., CEO, CFO, or CTO). In larger

organizations, the unethical behavior was a result of the lower level leadership's desire to hide information from the executive leadership team. In one example of this case, a participant described the VP as attempting to hide the actual results of the security report from the executive team, fearing that the report results would result in the loss of his job. The participant added that this VP ordered his director to generate the false report, which resulted in the orders being given to the security manager and in turn to the individual security professionals. The participant did share that his VP was eventually discovered to be ordering the alteration of the security reports and was immediately terminated for his actions. Insufficient evidence was collected to determine if organizational size was a determining factor in whether security professionals were either ordered to engage in or chose to perform in unethical behavior. However, the results of the study indicated that this behavior was experienced in both small and large organizations, suggesting that the size of the organization was not a factor.

All but one participant held at least one professional certification, and each of those participants expressed their fear of losing their certifications as a result of their unethical behavior. Several participants described having conversations with other security professionals with whom they worked and the actions they would undertake if their unethical behavior was discovered. In many instances, this driving tension led to resolution actions such as secretly documenting the unethical demands they were given. Several participants also described coordinated efforts by the team to protect each other in case of the discovery of one individual's unethical behavior. Part of the reason for this is that the discovery of one individual's unethical behaviors would cast light on the rest of the team's unethical behaviors; and in part as a means of assisting in the secret documentation of the unethical demands from their supervisors to avoid the detection of their clandestine documenting efforts.

Although all the participants understood their ethical obligations to properly generate security reports, regardless of having a professional certification outlining this obligation, they were individually forced to weigh the outcome of their actions against their ethical obligations. For instance, when confronted with a choice of either engaging in the unethical behavior being demanded of them by a supervisor or to refusing these demands because they violated the oath to undertake ethical behavior, they had to weigh the repercussions of these two choices. As the results indicated, the choice was most often to engage in the unethical behavior while using one or more forms of resolution actions such as simply denying the responsibility for their actions or secretly documenting the unethical demands as a means of justifying their actions. On the one hand, the individuals have a genuine fear of consequences for refusing the unethical demands, such as termination; on the other hand, they risk losing their professional certification. Additionally, for each choice, they must judge the time to consequence and the relative impact on themselves. The results suggested that the individuals believed that the more immediate consequence of reprisal for disobedience is often believed to be more certain than the more long-term consequence of potentially losing their professional certifications.

This study sought to identify the tensions that information security professionals experience in their reporting efforts and the actions they undertake to resolve those tensions. In this study, literal replication logic was used for gathering similar experiences from information security professionals, whereas theoretical replication logic was employed to ascertain if four different groups separated by experience and gender had diverse experiences that affected their information security reporting. Different experiences were described between the male and female participants, but these variances were limited to interactions between the two genders, indicative of gender bias or pay inequality. No evidence supported either of these differences between males

and females as having an effect on the accuracy of information security reporting. As such, this study did not find evidence to suggest that gender plays an important role in the accuracy of the information security reports generated.

Similar to gender, experience was not demonstrated to create significantly different reporting practices with the more experienced participants describing similar tensions as the inexperienced participants. This result underscores the common experiences by information security professionals as they progress in their careers. However, an exception in this case is the coercion described by the more experienced participants. This outcome is understandable as the less experienced security professionals are not expected to have the knowledge and experience required to refuse many of the unethical demands this study has described. Hence, the less experienced security professionals are more likely to comply with their leadership's demands even when those demands are considered unethical. On the contrary, the more experienced participants indicated a higher level of coercion used by their leadership, which engendered unethical behaviors under duress.

V.1 Paradoxical Tensions

In the participants' depictions of their experiences, several common themes emerged as drivers of tensions that they faced in their roles. These tensions were latent, existing inherently in the roles that the participants held or as they engaged in security reporting, and such tensions remained latent until they surfaced in specific information security reporting situations, at which point they became salient and needed to be resolved in one form or another by the security professional. These tensions do not resolve themselves but instead force the security professionals to reflect back on the tension as they act to resolve them, often creating a new tension to be addressed (Lewis, 2000; Putnam et al., 2016). Given this recurring evolution of a tension into a

new tension, security professionals engage in two or more resolution steps as they attempt to resolve the tensions. This case is especially true for security professionals as they encounter paradoxical tensions, whereby they are given unethical demands or realize they are in an unethical culture.

Unethical Security Culture

An unethical security culture is a culture where unethical practices have become common. These unethical practices are typically the result of prolonged unethical demands from the leaders as they attempt to hide information from the executive leadership of the organization. Nonetheless, this situation is not always true, as small organizations with poor or unethical security cultures often include the executive leaders who engage in making the unethical demands. For smaller organizations, this outcome often emanates from the executive leaders' desire to grow their business; furthermore, these executive leaders are willing to engage in unethical practices to achieve this goal. For larger organizations, these unethical demands stem from the lower to middle management's fear of looking bad to the executive leadership. These managers frequently demand that security reports be altered by their subordinates, fearing that the authentic results will in some way cause them to lose their jobs should the executives learn of the unaltered results. These unethical demands, once they become salient, subsequently develop into a paradoxical tension for the information security professional as they must now choose between two or more competing demands.

Information security professionals who engage in information security reporting do so against the backdrop that they undertake a practice that is intended to discover information security issues, and these issues are then reported to the organization to help with mitigating or remediating these security issues. Security-related issues cover a broad spectrum of threats to an organization,

which originate from internal and external sources and can be malicious or accidental. These same security professionals are expected to be ethical in their efforts, and they count on their organizations to foster an ethical security culture. However, as this study indicates, information security professionals often join organizations that appear to be ethical at first, but they quickly realize that they have entered into an unethical security culture as they are given demands that contradict or violate the organization's security policies, regulatory requirements, or industry standards. This situation creates a paradox as they are confronted with contradictory requirements (Lewis, 2000), that is, complying with their leadership's unethical demands or maintaining the policy requisites or industry standards they are being told to violate. This unethical security culture is frequently driven by leadership's desire to hide security information from the executive leaders. This concealment of information from the executive leaders often creates an unethical security culture that becomes undiscovered, as the unethical practices are used to hide this security culture from the executives. However, the study denotes that at times, such as within a small organization, the CEO is also responsible for this unethical security culture. Over time, as the leadership continues to make unethical demands of the security professionals, these unethical practices become common and the individual security professionals begin to engage in unethical practices, knowing that the practice is what is expected from their leadership. As this situation persists, the entire security culture becomes characterized by corrupt practices, which would require a major effort to correct. In resolving this tension, security professionals must deal with multiple paradoxical tensions, including the following: Should they comply with the unethical demands of their superior or maintain their ethical obligation and thus increase their chance to be terminated? Should they violate the ethical requirements of their professional certifications or engage in the unethical demands of their superior? Depending on their industry, security professionals may even

be faced with the paradox of engaging in the demand to alter reports that are used for achieving industry or regulatory certification or risking termination by notifying regulators about the unethical demands and unethical practices within the organization.

Fear of Looking Bad

Although a poor or unethical security culture is an overall culture issue that is due to unscrupulous practices that have become common from the prolonged unethical demands of leadership, the fear of looking bad is the most common driver that engenders these unethical demands. The leadership's fear of looking bad to the executives frequently stems from the security report showing a large number of findings. This trepidation drives the leadership to engage in the unethical practice of altering or manipulating the security reports prior to the reports being sent to the executive leadership. As attribution theory explains, individuals perceive their relationship between the cause of an issue and the outcome of that issue, with issues being either internal or external to those individuals (Munton et al., 1999; Park et al., 2008). This inference is evident in a case where the leaders fear that the report will have a negative effect on them directly and engage in unethical behaviors or order their subordinates to perform unscrupulous behaviors by altering the security reports. This fear of looking bad is not limited to the security leadership, but it can also exist between the stakeholders with whom the security professionals interact, as the stakeholders dread the effect that the security reports will have on them or their business unit. This situation creates a performance paradox where tension occurs between stakeholders with conflicting demands (Smith & Lewis, 2011). This tension is experienced as the information security professional must generate a security report using information provided by the stakeholder; however, the stakeholder's fear often results in the alteration of information, refusal to provide information, or attempts to convincing the security professional to avoid proper

reporting. The mum effect, which employs attribution theory as its theoretical background, indicates that two factors influence an individual's desire to report bad news. These factors are time effect and fault responsibility (Park et al., 2008). As the current study shows, security professionals often get the sense that a stakeholder is withholding information or has provided false information in an attempt to reduce the effect the security report will have on them. This case demonstrates fault responsibility; the more the stakeholders view themselves as not being at fault for the information they provide, the more likely they are to provide the information (Park et al., 2008). Stakeholders frequently wait until the end of a security audit or near the end of a deadline before providing the required information to the security professional. This situation illustrates an example of the time effect, whereby the stakeholders are less likely to provide the information if they perceive they have time to wait before they must provide it (Park et al., 2008). Both of these factors employed by stakeholders become tensions that the security professional must deal with and are often sensed by the latter. Such contradictory sense or feeling transforms the tension into a paradox (Lewis, 2000). As security professionals must contend with the often mixed messages they receive from the stakeholders (Lewis, 2000; Putnam, 1986), they are then confronted with the paradoxical tension of reporting the information they were provided while ignoring their feeling of accepting inaccurate information, or attempting to verify whether the feeling is genuine. Security professionals also experience this paradoxical tension as they are given demands by their leaders whose goal is to attract or retain future business with their client, whereas the client's goal is to obtain a certification. The client and the organization's leader are engaged in two different goals, thereby creating a performing paradox (Smith & Lewis, 2011) that exists between the two organizations, and placing the security professionals between the two parties; furthermore, security

professionals experience a third and different paradox of meeting their employer's demands or writing an accurate report.

Tight Deadlines or Scoping Issues

Tight deadlines and scoping issues are not uncommon in business. Budgetary constraints and lack of proper planning are two common reasons for tight deadlines with scoping issues, which are typically related to a general lack of knowledge prior to an engagement starting. For example, the number of security findings prior to the beginning of an engagement would be impossible to determine, and the scoping would have to be set using prior knowledge of similar engagements. However, once a scan is completed and far more findings are generated, the engagement is no longer scoped properly. This factor can have a negative effect on the accuracy of a security report, as the information security professional must now deal with this scoping issue. Tight deadlines and scoping issues often create paradoxical tensions for information security professionals, and in resolving these tensions, often produces new ones (Lewis, 2000). This case is demonstrated in the results of the current study, as participants who are engaged as security consultants are responsible for generating a security report within a specified time limit before the true scope of the engagement is realized. As security professionals engage in the assessment, they realize that far more security issues were found than were expected and would take much longer to validate and report than was provided for in the scope of the engagement. The security professionals are then confronted with an either/or decision as a paradoxical tension. If the security professionals choose to get the report properly validated and reported, their free time will be required, as they must work off the clock on their own time to meet the deadline. Otherwise, they can opt to validate as much as possible and generate a report that is inaccurate but is reflective of what they could do in the time they were provided. The two choices are a paradox because neither alternative offers a

positive outcome for the individual. As the study indicates, many security professionals make the choice to work on their own time to meet the deadline, which results in a new tension that they must deal with, consequently confronting them with potential health and relationship issues as they work to meet the deadline. For those security professionals who elect to submit a report that only shows what they had time to validate and does not cover the entire list of security issues found, they are now faced with the knowledge that the organization may not be asked to return in the future by that client. However, they did not sacrifice their own time in order to meet the poorly scoped deadline. This case is another example of a paradox created by contradictory demands (Lewis, 2000), as the security professionals had to decide between creating a fully accurate report and sacrificing their personal time to meet the deadline, or producing an incomplete report without sacrificing their personal time. This decision can be a very difficult one for security professionals with other obligations on their personal time, such as families, second jobs, and other external activities (e.g., volunteer work).

Lack of Experience or Knowledge

Lack of experience or knowledge is associated with stakeholders in the security teams and those stakeholders with whom they interact. It is primarily related to new security leaders with inadequate experience in managing a security team, but it can also be related to new security professionals who have recently entered the security field. Furthermore, lack of knowledge is associated with the stakeholders with whom the information security professionals must interact, including internal and external stakeholders. For new security leaders, security professionals confront this tension when working with inexperienced leaders, and such tension is often driven by the leaders' demands for the security professionals to engage in actions with which the latter does not agree. When leaders are new, they frequently adopt a conservative approach and set

demands or standards that may not be in the best interest of the client or the organization, but this approach is expected to be a safer one. Security professionals are faced with the paradox of deciding between doing what they are instructed to do despite their belief that it is not the best action, or defying the instructions and doing what they feel is best for the client or the organization. The security professional is confronted with the absurd and irrational existence of opposites that can simultaneously exist, whereby either choice is both right and wrong (Lewis, 2000). In ignoring their leader, security professionals believe that they are acting in the best interest of the client yet resisting their leader's instructions; by contrast, following the leader's instructions is required, but it may not be in the best interest of the client or the organization. In these examples, security professionals may possibly be both right and wrong regardless of their choice.

Another issue related to a lack of knowledge emerges when the security professional is expected to generate a security report but must also deal with obtaining information needed from stakeholders who do not know how to provide it. Security professionals must then decide between attempting to gather the information another way or reporting that the information was unavailable. This either/or decision creates the paradoxical tension (Lewis, 2000), and security professionals often resolve this tension based on how tight a deadline they are facing. When dealing with a stakeholder directly and in person, security professionals can often assist the stakeholder depending on the latter's willingness to be assisted; however, this case becomes more complicated if the stakeholder is only interacted with via email or phone conversation.

Perceptions of Security

Oftentimes information security professionals must deal with the stakeholders' perception of security as a roadblock or that they are perceived as being too demanding, and these perceptions affect how stakeholders interact with security professionals. As the study indicates, some

stakeholders attempt to bypass security professionals, thus reducing the security professional's ability to engage in their reporting efforts. As previously mentioned, the stakeholders' fear of the effects that a security report will have on them triggers a conflict between the stakeholder and the security professional, creating a performing paradox where tension occurs between stakeholders with conflicting demands (Smith & Lewis, 2011). An example of this paradoxical tension is an information security professional who must generate a report of the vulnerabilities in an application being developed for use by the organization. The security professional has a mandate to provide as accurate a report as possible, and the needs of the business unit are disregarded in this report. The business unit leader who is responsible for the development of this application has to meet a deadline that is set by their leadership. The business unit leader knows that any security findings in the security report will cause a delay in the final delivery of this application. As the two work for the same organization, a frequent assumption is that they are endeavoring toward the same goal; however, in reality, they have competing demands that further increase as the deadline looms for the business unit leader. As the deadline gets closer and security issues continue to be found by the security professionals, the more likely the business leader will view the security professional as a roadblock. For those business unit leaders who have already experienced this situation, they will engage with the security professionals from the outset, with the perception of security as an obstacle. For security professionals, they are simply doing their job of reporting the security issues in the application, but now they must also deal with the behaviors of the business unit leader who often will launch attempts at manipulating the information that is provided to the security professional. For the more experienced security professionals who are engaged in a leadership role, they will undergo a similar tension but for a different reason, as their security department falls under the same executive leadership of the CTO as the business units they are

responsible for providing security reports to. These leaders must compete against each other for budget and resources but with very different goals to achieve. As that budget is allocated by the CTO, it will often create conflict between the departments, further enhancing the negative views of security.

Team Politics

Team politics pertain to the behaviors exhibited by individuals as they interact with other team members, as very few information security roles involve working alone. This situation is demonstrated in the study, as all the participants have worked in a team setting during their careers. Except for one participant, all the participants continue to have roles as part of a team. The more experienced participants often progressed from being in a team member role to a supervisor role, with one participant having started his own information security consulting company. As the owner of his own company, this participant often hires contract personnel, subsequently assuming the role of a team leader. Teams are predominant in the information security field; hence, the fact that many teams are forced to deal with team politics is not surprising. However, dealing with team politics is also deemed to influence security reporting. The study indicates that some information security professionals intentionally alter security reports in an attempt to sabotage their supervisors or deny access to other security professionals who request access to training or documentation required to write a security report.

These actions generate a performing paradox (Smith & Lewis, 2011), whereby security professionals are expected to create an accurate security report, but they decide to perform unethically in an attempt to discredit their manager. The paradox is not experienced by security professionals engaged in the unethical behavior but by the security manager and other security professionals on the team as they learn about the unethical behavior. Once the issue is resolved,

they are now confronted with a changed world where they can no longer trust this security professional to act ethically. Security managers must choose between continuing to lead their team as before assuming the incident was a unique occurrence or changing the way they manage in an attempt to prevent the situation from recurring. Team politics do not always involve unethical behavior; in fact, it is often demonstrated by team members who neglect their duties, causing other team members to shoulder the additional burden. As a result, these other team members have less time to perform their own tasks, which can affect the security reports.

Coercion

Coercion is more than simply making a demand of security professionals; it involves threatening the individual or others as a means of forcing security professionals to engage in behaviors they would not otherwise engage in. Information security professionals are often confronted with coercion; the less experienced security professionals experience milder forms of coercion, such as stakeholders' attempt to convince the security professional to alter a report by adding some form of fear (i.e., being afraid that they would lose their job if the security professional were to submit their reports as it is). The more experienced security professionals become, and as their role moves into a leadership role, the coercion becomes more pronounced and often involves threats to others. As the study indicates, security professionals are often willing to defy the unethical demands when the threat is individually directed to them; however, when the coercion involves threats to others, security professionals are inclined to engage in unethical behavior, as their leadership is demanding. The paradoxical tension is a choice between complying with organizational policies, regulatory requirements, and industry regulations, which presents a potential to cost others their jobs, or conforming to the unethical demands being set by the security leadership. The paradox that security professionals confront is exaggerated by the knowledge that

others are now being influenced by the outcome of their decision. Described in the section on improving information security compliance, the use of the neutralization technique of "defense of necessity" is employed by individuals to rationalize their deviant behavior whenever necessary. However, similar to all seven of the neutralization techniques, the defense of necessity is a self-realized rationalization, and its use does not involve outside individuals. Neutralization techniques may be employed by individuals to rationalize their deviant behavior; nevertheless, this rationalization is a purely internal mechanism adopted by the will of the individuals on themselves, and it is not forced upon them by an outside actor. As this study demonstrates, security professionals who are forced to confront coercive actions involving a threat to others are obliged to act under duress. Duress is a legal term that is heavily contested in the criminal justice field as either being no different from the defense of necessity or being a unique defense that a reasonable person would be unable to resist and should be understood as being situational and not dependent on the threat being manmade or natural (Westen & Mangiafico, 2004). In his article titled "Techniques of Neutralization: A Reconceptualization and Empirical Examination," W. William Minor conceptualized the seventh neutralization technique that he referred to as the "defense of necessity;" this technique denotes that if the security professionals perceive the unethical behavior as necessary, then they need not feel guilty of this moral conflict (Minor, 1981). This concept is in holding with the conservative criminal justice belief that a defense of necessity should be the same for a man-made threat as it is for a natural threat such as being obliged to take action that would otherwise be illegal as a means to prevent an even more egregious illegal act. By contrast, the liberal conservative view argues that the Model Penal Code suggests that individuals should be afforded a defense to threats that they would be unable to resist (Westen & Mangiafico, 2004). This liberal view is supported by the Model Penal Code Section 2.09. Duress, which clearly states

that an actor has an affirmative defense when engaged in conduct that would be an offense because he was coerced to do so by the use of force or the threat of force against himself or against another and this person was of reasonable firmness in his situation would have been unable to resist (Model Penal Code, Sec. 2.09(1)). Arguably, information security professionals should be considered as persons of reasonable firmness in their situation, given their overriding obligation to defend against the highly deviant behavior in which they must engage. However, security professionals who perform unethical behavior under duress have not necessarily compromised their status as responsible individuals, but this understanding does challenge if the security professionals are responsible for the unethical act (Brink, 2018). Furthermore, the security professionals' justification in their actions is not simply a matter of social reality but is solely an issue of their beliefs (Fletcher, 1998). Much of the current understanding of behavioral information security is derived from the criminal justice field; hence, a reasonable argument is that a discussion should begin among scholars in the behavioral information security field of the separation between Minor's "defense of necessity" and the malicious behavior under duress. As previously explained, there is support among criminal justice scholars and the Model Penal Code for this new category of neutralization technique.

V.2 Resolution Actions

Similar to how information security professionals often deal with more than one tension at a time, they also frequently engage in multiple resolution actions simultaneously as they attempt to resolve one or more tensions. Additionally, many resolution actions are used for different tensions confronting information security professionals (see Figure 3).

Figure 3:
Mapping of resolution actions to paradoxical tension

Drivers of Tensions	Resolution Actions
Unethical security culture	Attempts to change the organization Denying responsibility Self-protection Forming tight subgroups Repressing the tension Withdrawing from the tension
Fear of looking bad	Denying responsibility Self-protection
Tight deadlines or scoping issues	Denying responsibility Forming tight subgroups
Lack of experience or knowledge	Self-education Denying responsibility
Perceptions of security	Forming tight subgroups Attempts to change the organization
Team politics	Forming tight subgroups Self-education
Coercion	Repressing the tension Self-protection Withdrawing from the tension

Denying Responsibility

As information security professionals attempt to confront the tensions associated with a poor or unethical security culture, a fear of looking bad, tight deadlines and scoping issues, or the lack of experience or knowledge, they often choose to deny responsibility for their unethical

behavior in altering a security report. This resolution action was commonly undertaken by the less experienced security professionals in this study. Security professionals rationalize their actions as being the responsibility of their leadership; moreover, they assert that their actions are forced on them, which constitutes a neutralization technique referred to as the "denial of responsibility" (Sykes & Matza, 1957). This assertion of responsibility is frequently accurate, as the less experienced security professionals lack the experience or knowledge required to act against their leadership's unethical demands. In the current study, the less experienced security professionals without one or more professional certifications primarily adopted this resolution technique, doing so with little to no additional coercion required from their leadership. By contrast, the more experienced security professionals similarly described the use of this resolution technique early in their careers; however, as they gained experience, they began to refuse engaging in the unethical behaviors that their leaders had demanded of them. The difference between the experienced and inexperienced security professionals suggests that over time, as experience is gained, security professionals are less likely to perform unethical behavior even when confronted with the demand. This knowledge becomes important for security professionals who are early in their careers because they are more likely to be hired by organizations with poor security cultures as they attempt to gain experience with firms that know they can pay less for this lack of experience.

Attempts to Change the Organization

Attempts to change the organization were made as resolution actions when dealing with the paradoxical tensions for an unethical security culture and the perceptions of security that security professionals must deal with. Both security professionals having less experience and the ones with more experience described attempts to change the organization after realizing they were in an unethical security culture or were having unethical demands placed on them by their

leadership. Such efforts to resolve a persistent tension were largely employed by the more experienced security professionals, whereas several of the less experienced professionals made similar attempts but to a lesser degree. This finding suggests that as security professionals gain experience, they are more likely to engage in creating an ethical security culture. When dealing with the other stakeholders' perceptions of security professionals as a roadblock or as excessively demanding, the more experienced security professionals would undertake efforts to change those perception by directly engaging the stakeholders to highlight their department's demands in an attempt to demonstrate that their actions were in alignment with the business unit leadership. The more experienced participants would frequently describe efforts to work with the stakeholders to help them to achieve their own goals. In one example of this case, an experienced security manager advised that he would offer to allow some middle ground to be attained, thereby permitting the business unit to continuously function while resolving the remaining issues. This effort was not strictly in keeping with a security policy, but it served to alter the perception of security as a roadblock. The less experienced participants demonstrated attempts to change the organization by advising the leadership about the regulations and how the organization was failing to meet those regulations. Such counsel would frequently fall on deaf ears, and the security professional would then engage in whatever behavior was being demanded. This incident demonstrates that even early in their careers, most security professionals make attempts to change their organizations for the better.

Self-protection

This resolution action is undertaken when security professionals are confronted by several paradoxical tensions, including an unethical security culture, fear of looking bad, and coercion. When faced with the realization that their organization or leaders are engaging in unethical

behaviors, security professionals begin to take actions designed to protect themselves in the event that their actions are discovered. This case is typically illustrated in the security professionals' decision to keep notes or documentation that provides evidence of their unwillingness to participate in the unethical behavior that is being demanded of them. Many security professionals conceal these notes from their leadership, depending on the level of fear they have for the potential repercussions of being discovered. Security professionals who are new to their careers often request their leaders to confirm their demands via an email as a means of recording their leaderships orders that they have deemed to be unethical. The severity of the unethical demand dictates the type of documentation that the security professional uses. In an example of this case, a manager orders a security analyst to decrease the severity of a finding without having a justifiable reason for doing so. The security analysts frequently request a confirmation of the instructions to save as proof that the reduction of the severity level is at the manager's behest and that they are not acting on their own. A more severe example of this situation involves a security manager who orders to alter a security report to remove issues and eventually reduce the report's impact. The security manager typically keeps the original report and sends the altered report as instructed. Keeping the original document then serves as proof that the security professionals created an honest report yet were ordered to alter or manipulate the data in the final report. Whatever the means used, security professionals at all levels of experience engage in self-protection when confronted with unethical demands. This resolution type is a delayed form of projecting where should the unethical behavior become known, the security professionals then expects they can use this evidence of their reluctance to shift the blame to another responsible party (Lewis, 2000; Putnam et al, 2016).

Self-education

When faced with a paradoxical tension related to the lack of experience or team politics, security professionals often engage in self-education to resolve these tensions. When security professionals experience a tension that is designed to block them from completing their job such as being blocked from training or from documentation that will assist them in their reporting responsibilities, they frequently resolve this tension by self-educating. This resolution technique is a form of repression, whereby security professionals choose not to directly engage in resolving the tension and instead ignore it by educating themselves in their own time (Jarzabkowski & Lê, 2016). In the current study, this move was more often described as a resolution action undertaken by the less experienced security professionals and was generally related to their fear of their inexperience, causing their fellow team members to suffer management's anger at not meeting certain demands. When security professionals are new to the industry, they normally realize that their formal education has not taught them what they need to perform their job function, or that they need to achieve a professional certification if they intend to advance in their careers. Oftentimes organizations do not offer additional assistance in this area, and security professionals must rely on themselves to achieve their goals. When team politics are the source of tension, security professionals must work outside of the team and often outside of the organization to gain the knowledge they require to perform their responsibilities. As the security field is a constantly changing space, most information security professionals tend to be self-educators; when confronted with these two tensions early in their careers, many quickly move to self-educate.

Forming Tight Subgroups

Security professionals working in a team typically have shared experiences. They may individually experience unethical demands but working as a team facilitates the sharing of the

stress that these demands induce. As a result, a resolution type known as splitting transpires, in which the team becomes a subgroup that forms a we/them distinction as the team members attempt to deal with management's demands, thus creating a distinct social divide (Lewis, 2000; Smith & Berg, 1997). The group frequently engages in social activities such as going to lunch or having drinks together, and the members exclude the leadership from these events. Furthermore, security professionals in the group often engage in informal discussions related to the unethical practices that their leaders are demanding of them and how those demands may affect their professional certifications. As a group, security professionals discuss resolution actions such as self-protection and they begin documenting their leadership's unethical demands. Instead of acting as individuals attempting to make change in the organization, the group acts in a concerted manner and discusses its efforts. In this way, each individual security professional will not attempt resolution actions, but every member of the group will undertake a different resolution action and the remaining members will accept the result for the group. As a group, security professionals act to protect each other against their leadership. This approach is particularly effective as the team documents the unethical demands of each group member, preventing their leadership from discovering their documenting actions. When the group includes a supervisor such as a team lead or manager, the documentation typically resides with this individual as the informal leader of the tight subgroup.

Repressing and Withdrawing from the Tension

When security professionals attempt to resolve the paradoxical tensions, including working in an unethical security culture or coercion through other means such as attempting to change the security culture of the organization, and those attempts have failed, they generally engage in two resolutions actions simultaneously. First, they repress the tension by ignoring or denying the existence of the paradoxical tension (Jarzabkowski & Lê, 2016). This resolution action is used as

a short-term solution as they attempt to withdraw from the tensions that they were unable to resolve. Security professionals go into a survival mode where they have given up and are simply trying to do enough not to be noticed. They then lose all the respect for their leadership and often for the company. Security professionals repress the tensions, believing that any additional efforts to resolve the tension will fail. At this point, security professionals have decided that no other alternatives to resolve the tensions are available and thus begin seeking employment at another organization. When this situation involves security professionals who are part of a tight subgroup, their departure is usually followed closely by others from the same subgroup as the support network starts to break up. This event is an important one for upper management to take note of because it may verify that an unethical security culture exists within the organization, which needs to be resolved. If the security professionals are unable to find another role at another organization, they continue to repress the tensions until they are able to withdraw from the organization. As time passes, these security professionals become more withdrawn from coworkers and reduce their interaction with their leadership.

V.3 Conclusions

Information security professionals are not exempt from acting in an unethical manner as it relates to information security reporting. These unethical practices, regardless of their origin, create a paradox for the organization that must rely on these security reports. Even the ethical or conduct requirements of the professional certifications do not prevent security professionals from engaging in unethical behavior despite fearing the consequences of losing their certifications or long-term career aspirations.

In the subsequent sections, the drivers of tensions that information security professionals experience and the resolutions actions they use for resolving those tensions that lead to dealing

with paradoxical tensions, are described. The contributions of this study to practice and to theory as well as the study limitations and suggestions for future research are also presented.

Drivers of Tensions

Security professionals encounter and need to resolve several drivers of tensions; in resolving these tensions, they are then forced to resolve another tension triggered by the resolution actions of the original tension (Lewis, 2000; Putnam et al, 2016). As the present study indicates, the action of dealing with a driver of tension frequently creates a paradoxical tension, whereby the information security professional must decide between two or more competing obligations. This study provides evidence that despite the best intention of information security professionals, the security reports they generate may not be as accurate as expected and are often intentionally altered. Regardless of the reason for altering the report, normally it does not represent the true security picture to the executive leadership. This situation poses a problem for the organization's leaders who are often unaware of the unethical practices occurring in their security department; furthermore, most of the unethical practices are being demanded by senior and middle managers who ensure that the executive leadership is kept unaware of such practices. Notably, unethical practices are not universal to every organization. In this study, the more experienced security professionals described their departure from organizations that engaged in unethical practices and in time managed to find an organization that upholds an ethical security culture. Once these security professionals find an ethical organization, they typically remain with that organization much longer than they did at previous unethical organizations. This turnover, especially of security managers, may be a signal to executive leaders that they have a poor or unethical security culture that needs to be eliminated and fixed.

Resolution Actions

As security professionals resolve the paradoxical tensions they encounter, they engage in a number of resolution techniques, often moving from one to another as the tension is resolved and a new tension emerges (Lewis, 2000; Putnam et al, 2016). The progression of resolution steps that the information security professional adopts usually depends on the level of experience the security professional has at the time. The less experienced security professionals often simply deny their responsibility by shifting any blame for their unethical behavior to their immediate leadership who gave the order to engage in this behavior. As security professionals gain experience, they begin to refuse these unethical demands and attempt to make changes to their organization to transform the security culture from an unethical to an ethical one. They frequently initiate the secret documentation of the unethical demands and practices that they take part in or observe. They also often engage an outside party such as HR or the internal audit teams; however, this approach oftentimes does nothing to stop or change the behaviors. Even when a method of anonymous reporting of this unethical behavior is available, security professionals fear their participation in the unethical practices because they likewise engage in them at the leadership's behest. Moreover, despite the team of security professionals' establishment of a tight group as a coping mechanism, the eventual departure of one member leads to the departure of most if not all of the remaining members. For the executive leadership, this factor may also be a useful indicator of a poor or unethical security culture. When the majority of a security team leave over a brief period, the leadership should recognize this occurrence as a red flag of a problem that the middle management may be hiding.

V.4 Contribution to Practice

As this study indicates, many reasons underlie a security professional's alteration of a security report. From an organizational viewpoint, the information security professional is expected to act in an ethical manner and in the best interest of the organization. However, this study has highlighted seven drivers of tensions that lead to the altering of security reports by security professionals. By considering these drivers of tensions and the resolution actions, an organization can initiate efforts to mitigate these tensions and thus reduce the likelihood of security reports being altered. An example of this case is the mass departure of security staff. As the study shows, security professionals who are forced to engage in unethical behavior often form tight subgroups that serve to protect the group against the leadership making the unethical demands. When one member of the subgroup chooses to leave the organization, the remaining members normally leave soon after as the protection that the subgroup created has been reduced. This mass exodus of a security team should raise a red flag for the executive leadership because the incident may imply that all resolution efforts have been exhausted by the security professionals and the final resolution attempt is to remove the tension by leaving the organization.

The fear of looking bad is not uncommon for most organizations as the most typical method of managing is failure intolerance. In other words, individuals fear failing because of the potential repercussions of failure. In this study, several participants explained that unethical demands were given by their leaders because of the latter's fear of being viewed as having failed. As it relates to a security organization or a business unit, a failure-tolerant culture may be more appropriate to avoid the fear of failure leading to unethical behaviors. In a failure-tolerant environment, leaders are allowed to fail, with the understanding that failure will increase the understanding of why they failed, thus resulting in the avoidance of the same failure in the future. Many of the experiences

and the resulting drivers of tensions described by the participants could have been significantly reduced or even eliminated by a failure-tolerant environment.

Numerous companies have adopted an open-door or an anonymous reporting policy designed to encourage personnel to report unethical behaviors or demands to the organization. As the study indicates, these policies and practices do not work. One participant was accused of having reported a violation that was supposedly anonymous. Although the individual did not make the report, the incident clearly demonstrated to him that nothing was truly anonymous; furthermore, he realized that had he decided to file a report of the unethical demands, this action would result in termination. Several other participants described fears related to the reporting of ethical violations because they would be included with those who were making the unethical demands. Even when secretly documenting the unethical demands and ethical violations, the participants did not report the issue to the organization or regulatory bodies for fear of being associated with those engaged in the unethical behavior. A possible solution to this dilemma is to include a middle agent in the reporting effort. An example would be to engage a professional certification organization to submit the ethical violation. The certification organization could then report the violation to a regulatory body or governmental agency for investigation, allowing for the protection of the individual. Regardless of the mechanism for reporting these issues, the current method is neither effective nor capable of reducing the unethical demands and behaviors noted in this study.

V.5 Contribution to Theory

Organizations rely on information security professionals to identify and report on the security issues that need to be mitigated or remediated to acceptable levels and thus strengthen the organization’s security posture. These information security professionals are expected to conduct themselves in an ethical manner as they endeavor to combat the accidental and often intentional

security threats that can be internal or external to their organizations. Their efforts are normally driven by industry and regulatory requirements such as the regulatory requisites to protect the personal health information of patients or the credit card information of consumers. The primary means of determining the effectiveness of these security efforts is the security report that is generated by information security professionals themselves. This study provides evidence that a paradox exists in the creation of these security reports. The paradox is that the very security professionals an organization relies on to protect and report on the effectiveness of the security efforts are often manipulating the security reports they create to prevent the real security effectiveness from being shown to the executive leadership. Information security professionals do not desire to alter or manipulate the security reports they generate, but they are frequently ordered to do so by their leadership. As a result, they must resolve the ensuing paradoxical tension that in turn creates a paradox for the organization, as it must rely on these reports to protect against the threats that it faces.

This paper contributes to paradox theory by demonstrating the paradoxical tensions that information security professionals must deal with as they engage in security reporting and the resolution actions used in addressing these paradoxical tensions. In doing so, this paper contributes to behavioral information security in two areas. First, it adds to the understanding of the difference between insider deviant behavior and insider misbehavior, which serves to improve information security compliance by highlighting the unethical behaviors engaged in by information security professionals, to include the causes of this unethical behavior and the resolution steps that the security professionals undertake. Second, the study presents a conceptualization of a new category of neutralization technique used by information security professionals in resolving paradoxical tensions as insiders who perform deviant behavior under duress.

Distinguishing Between Insider Deviant Behavior and Insider Misbehavior

As this study has indicated, information security professionals understand their roles and the ethical requirements for accurate security reporting. However, they often engage in the unethical practice of altering or manipulating security reports that are given to the executive leadership. Although information security professionals intentionally engage in this unethical practice, they frequently do so at the behest of their leaders, thereby creating a paradox as they are confronted with contradictory demands (Lewis, 2000).

The present study identifies seven tensions that security professionals often deal with, which engender unethical practices when generating security reports. These tensions are poor or unethical security cultures, fear of looking bad, tight deadlines or scoping issues, lack of experience or knowledge, perceptions of security, team politics, and coercion. A security professional normally deals with more than one of these tensions simultaneously, and these tensions are oftentimes the driving force that leads to the manipulation of security reports. This study also identifies seven resolution actions that security professionals undertake when attempting to resolve the tensions. These actions are denying responsibility, attempting to change the organization, self-protection, self-education, repressing the tension, forming tight subgroups, and withdrawing from the tension.

By understanding the unethical behaviors and their underlying motivations, this study has increased the body of knowledge toward improving information security compliance. Information security professionals are privileged insiders who engage in roles and responsibilities that put them in a position to cause more harm to an organization than non-security insiders. Policies and regulations continue to be created based on attribution theory. However, as this study underscores, these policies and regulations are being ignored as information security professionals are being

forced to resolve the paradoxical tensions between the rules and regulations and their leadership's immediate demands that contradict or violate these rules and regulations. This situation becomes even more pronounced as security professionals gain experience in their career and begin to move into leadership roles as the more extreme forms of coercion arise. This inference leads us to our second contribution to theory.

Insider Deviant Behavior Under Duress

As this study indicates, information security professionals encounter different levels of coercion as they progress through their career. This experience is normally demonstrated as a minor form of coercion, which is easy to resolve; an example involves stakeholders trying to use coercive rhetoric to convince a security professional to make changes to a security report. The more experienced security professionals who have moved into leadership roles undergo more extreme forms of coercion from their senior leaders, which almost always involve some threat that is intended to put them under duress. This approach is in contrast to Minor's "defense of necessity," which can include situations such as a security professional claiming that he was not given sufficient time to complete his report, thus necessitating his generation and submission of an incomplete report. Defense of necessity does require the use of a threat, and this aspect is the defining difference between the defense of necessity and malicious behavior under duress. Two elements are always present when a malicious act is committed under duress. First, a threat is made and is most often directed toward others, but it can be made directly at the security professional. Second, the threat is not internal, but rather is always external, signifying that the security professional is not simply assuming that a threat exists. This threat typically comes from external sources such as senior leaders. When confronted with a threat that is being directed toward others, security professionals are less likely to choose to follow the rules or regulations. The reason is that

they determine the threat to be more likely to occur than the organization is to be caught violating a rule or a regulation. Additionally, security professionals recognize the threat as having a greater impact on the lives of those who are being threatened than a potential fine to the organization will have. By understanding that security professionals confront this type of dilemma, we begin to understand how attribution theory may not be the best tool for designing policies and regulations that are meant to deter this type of deviant behavior. This study has provided evidence to support this assertion, as the experiences of the information security professionals demonstrate.

V.6 Limitations and Future Research

Limitations

This study used both literal and theoretical replications to generate a diverse population. However, all the participants lived in or had recently relocated from the Southeastern United States. As such, the participants' experiences may not be representative of the ones that information security professionals have in other parts of the country or in other parts of the world, as the difference in cultures may have an impact on how individuals perceive the world they live in and the tensions they experience. Additionally, this research focused on one area of the information security field, security reporting, which did not represent the entire population of information security roles. Other information security roles may possibly have different experiences that are different from the ones depicted by the participants.

This study included eight participants. Although using a literal replication ensured that all of them were from the same field and were expected to have similar experiences, this limited sample size may not represent a complete picture of the experiences of a larger number of information security professionals. Additionally, this study did not find evidence to support a difference in experiences between male and female information security professionals as it affects

information security reporting, but the study did find that females often experienced gender bias and pay inequality. No evidence was provided to suggest that these factors had an effect on the participants' security report behaviors. Nonetheless, increasing the sample size or recreating the study using a different group may provide diverse results.

Future Research

This study answered a call for additional research into behavioral information security, namely, to improve information security compliance and the separation of insider deviant behavior from insider misbehavior. In answering this call, the author conceptualized a new category of neutralization technique, the malicious behavior under duress, and outlined two characteristics of its existence that define its separation from the "defense of necessity." Further research into information security professionals who have experienced being placed under duress conditions to force their compliance with the unethical demands of their leadership would be beneficial to the behavioral information security field. To the best of the author's knowledge, this study is the first work to focus on the behaviors of information security professionals as they engage in information security reporting. Further research into these professionals may help to illuminate the additional drivers of tensions that they experience, which result in paradoxical tensions. Furthermore, security reporting is only one aspect of information security; although it covers a broad range of potential security roles, it does not encompass the entire range of roles in the information security field. Expanding this research to include other information security roles may be beneficial to understand if the experiences from this study are similar to the ones experienced by those in other security roles.

The size of an organization and the different levels of management within an organization were not a focus of this research, and these factors may have had an impact on the results. The

larger an organization, the more likely it is to have multiple levels of leadership above the individual information security professional. This study included participants from small organizations with 25 or fewer employees and large organizations with over 10,000 employees; however, this aspect was not tracked in the study. The size of the organization apparently lacked an impact on the results; nonetheless, a study using organizational size as a variable may determine if organizational size has an influence on the drivers of tensions or the behaviors of information security professionals as they engage in security reporting.

The second area addressed in this research was information security compliance; the results implied that information security professionals who are responsible for protecting their organizations often engage in the same unethical behavior that they are tasked with defending against. Although this study focused on information security reporting, further research into other security roles would serve to highlight the unethical behaviors that other security roles may be engaging in. In addition to other security roles, improving the understanding of how different regions and cultures from around the world are experiencing these unethical practices would increase the body of knowledge, thereby allowing management to develop better compliance requirements and analytics to detect these unethical practices and discover unethical security cultures that may be hidden from the executive leadership.

Further research into the impact of professional certifications on ethical behavior is important to understand the level of consequence to the individuals that may prevent or reduce the occurrences of violating their ethical or conduct requirements. The issue of whether a professional certification reduces the likelihood of individuals from engaging in unethical behaviors that are demanded of them by their leadership also merits an investigation. Gaining an enhanced understanding of these points can help to improve the deterrence language used by professional

organizations offering professional certifications to encourage compliance. Another area of interest for organizations is the identification of specific professional certifications that may increase ethical behavior. Such approach would assist an organization in determining the professional certifications that are most important to them when recruiting security talent or promoting talent within the organization into supervisory positions that may create a more ethical security culture.

REFERENCES

Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems and security incident responses. International Journal of Information Management, 35(6), 717–723. doi: 10.1016/j.ijinfomgt.2015.08.001

Ajzen, I. (1991). The Theory of Planned Behavior. Organizational Behavior & Human Decision Processes, 50(2), 179. https://doi.org/10.1016/0749-5978(91)90020-T

Alase, A. (2017). The Interpretative Phenomenological Analysis (IPA): A Guide to a Good Qualitative Research Approach. International Journal of Education and Literacy Studies, 5(2), 9–19. doi: 10.7575/aiac.ijels.v.5n.2p.9

Blakley, B., Mcdermott, E., Geer D. (2001). Information security is information risk management. In NSPW ’01: Proceedings of the 2001 workshop on New paradigms, pages 97–104, New York, NY, USA, 2001.ACM

Boland, R. J. Jr. "Phenomenology: A Preferred Approach to Research in Information Systems," in Research Methods in Information Systems, E. Mumford, R. A. Hirschheim, G. Fitzgerald, and A. T. Wood-Harper (eds.), North-Holland, Amsterdam, 1985, pp. North-Holland, Amsterdam, 1985, pp. 193-201. 193-201.

Boland, R. J. Jr. "Information System Use as a Hermeneutic Process," in Information Systems Research: Contemporary Approaches and Emergent Traditions, H-E. Nissen, H. K. Klein, and R. A. Hirschheim (eds.), North-Holland, Amsterdam, 1991, pp. 439-464.Jackson, C., Vaughan, D. R., & Brown, L. (2018). Discovering lived experiences through descriptive phenomenology. International Journal of Contemporary Hospitality Management, 30(11), 3309–3325. doi: 10.1108/ijchm-10-2017-0707

Brink, D. O. (2018). The Nature and Significance of Culpability. Criminal Law and Philosophy, 13(2), 347-373. doi:10.1007/s11572-018-9476-7

Calabretta, G., Gemser, G., & Wijnberg, N. M. (2016). The Interplay between Intuition and Rationality in Strategic Decision Making: A Paradox Perspective. Organization Studies, 38(3-4), 365–401. doi: 10.1177/0170840616655483

Cho, Sunyoung, et al. "Crossing the Diffusion Chasm: from Invention to Penetration of a Telehealth Innovation." Information Technology & People, vol. 22, no. 4, 2009, pp. 351–366., doi:10.1108/09593840911002450.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. Computers & Security, 32, 90–101. doi: 10.1016/j.cose.2012.09.010

Cybersecurity Insiders. (2019). 2020 Insider Threat Report (pp. 1–24). El Segundo, CA: Gurucul.

Denison, D. R., Hooijberg, R., & Quinn, R. E. (1995). Paradox and Performance: Toward a Theory of Behavioral Complexity in Managerial Leadership. *Organization Science*, *6*(5), 524–540. doi: 10.1287/orsc.6.5.524

Dictionary.com, LLC. (2020). Dictionary.com. Retrieved March 15, 2020, from https://www.dictionary.com/

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. The Academy of Management Review, 14(4), 532. doi: 10.2307/258557

Elifoglu, I. H., Abel, I., & Taşseven, Ö. (2018). Minimizing Insider Threat Risk with Behavioral Monitoring. Review of Business, 38(2), 61–73.

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. Security and Communication Networks, 9(17), 4667–4679. doi: 10.1002/sec.1657

Faems, D., & Filatotchev, I. (2018). Navigating a Dialectical Journey on Paradox Research: An Introduction to the Point-Counterpoint on Paradox Theory. Journal of Management Studies, 55(8), 1488–1489. doi: 10.1111/joms.12404

Farjoun, M. (2010). Beyond Dualism: Stability And Change As A Duality. Academy of Management Review, 35(2), 202–225. doi: 10.5465/amr.2010.48463331

Fletcher, G. P. (1998). Dogmas of the Model Penal Code. Buffalo Criminal Law Review, 2(1), 3-24. doi:10.1525/nclr.1998.2.1.3

Ford, J. D., & Ford, L. W. (1994). Logics of Identity, Contradiction, and Attraction in Change. The Academy of Management Review, 19(4), 756. doi: 10.2307/258744

Ford, J. D., Ford, L. W., & Damelio, A. (2008). Resistance to Change: The Rest of the Story. Academy of Management Review, 33(2), 362–377. doi: 10.5465/amr.2008.31193235

Giorgi, A et. al. (2017). The Descriptive Phenomenological Psychological Method. In C. Willig and W. Stainton-Rogers (eds.). The Sage Handbook of Qualitative Research in Psychology, 2e (pp. 176-192). Sage Inc.

Isc2.org. (2020). Code of Ethics: Complaint Procedures: Committee Members. Retrieved July 20, 2020, from https://www.isc2.org/Ethics

Isc2.org. (2020). Women in Cybersecurity. Retrieved July 19, 2020, from https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx?la=en&hash=270117229EA39FA1E7134CFB1C5BB1ACBDF8A88C

Jarzabkowski, P. A., & Lê, J. K. (2016). We Have To Do This and That? You Must be Joking: Constructing and Responding to Paradox Through Humor. Organization Studies, 38(3-4), 433–462. doi: 10.1177/0170840616640846

Kan, M. M., & Parry, K. W. (2004). Identifying paradox: A grounded theory of leadership in overcoming resistance to change. The Leadership Quarterly, 15(4), 467–491. doi: 10.1016/j.leaqua.2004.05.003

Klein, H. K., & Myers, M. D. (1999). A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. MIS Quarterly, 23(1), 67. doi: 10.2307/249410

Klockars, C. B. (1975). The professional fence (1st ed.). London: Tavistock Publications.

Lee, J., Bagchi-Sen, S., Rao, H. R., & Upadhyaya, S. J. (2010). Anatomy of the Information Security Workforce. IT Professional, 12(1), 14–23. doi: 10.1109/mitp.2010.23

Leonard-Barton, D. (1992). Core capabilities and core rigidities: A paradox in managing new product development. Strategic Management Journal, 13(S1), 111–125. doi: 10.1002/smj.4250131009

Lewis, M. W. (2000). Exploring Paradox: Toward a More Comprehensive Guide. The Academy of Management Review, 25(4), 760–776. doi: 10.2307/259204

Manen, M. V. (2016). Phenomenology of practice: meaning-giving methods in phenomenological research and writing. London: Routledge, Taylor & Francis Group.

Merleau-Ponty, Maurice. Phenomenology of Perception. Translated by Donald A. Landes, Routledge, 2012.

Miles, M. B., Huberman, A. M., & Saldaña Johnny. (2014). Qualitative data analysis: a methods sourcebook (3rd ed.). Los Angeles: SAGE.

Minor, W. W. (1981). Techniques of Neutralization: a Reconceptualization and Empirical Examination. Journal of Research in Crime and Delinquency, 18(2), 295–318. doi: 10.1177/002242788101800206

Model Penal Code, Sec. 2.09(1).

Moustakas, C. (1994). Phenomenological research methods. Thousand Oaks: Sage Publications.

Munton, A. G. (1999). Attributions in action: a practical approach to coding qualitative data. Chichester, West Sussex: John Wiley & Sons.

Orlikowski, W. J., and Baroudi, J. J. "Studying Information Technology in Organizations: Research Approaches and Assumptions," Information Systems Research (2:1), 1991, pp. 1-28

Park, C., Im, G., & Keil, M. (2008). Overcoming the Mum Effect in IT Project Reporting: Impacts of Fault Responsibility and Time Urgency. Journal of the Association for Information Systems, 9(7), 409–431. doi: 10.17705/1jais.00163

Polkinghorne, D. E. (1989). Phenomenological research methods. In R. S. Valle & S. Halling (Eds.). Existential phenomenological perspectives in psychology (pp. 41–60). New York Plenum.

Putnam, L. L. (1986). Contradictions and paradoxes in organizations. In L. Thayer (Ed.), Organization communications: Emerging perspectives: 151-167. Norwood, NJ: Ablex Publishing.

Putnam, L. L., Fairhurst, G. T., & Banghart, S. (2016). Contradictions, Dialectics, and Paradoxes in Organizations: A Constitutive Approach†. *The Academy of Management Annals*, *10*(1), 65–171. doi: 10.1080/19416520.2016.1162421

Seidman, I. (2013). *Interviewing as qualitative research: a guide for researchers in education and the social sciences* (4th ed.). Columbia University, NY: Teachers College Press.

Schad, Jonathan, et al. "Paradox Research in Management Science: Looking Back to Move Forward." Academy of Management Annals, vol. 10, no. 1, 2016, pp. 5–64., doi:10.5465/19416520.2016.1162422.

Seo, M.-G., & Creed, W. E. D. (2002). Institutional Contradictions, Praxis, and Institutional Change: A Dialectical Perspective. The Academy of Management Review, 27(2), 222. doi: 10.2307/4134353

Singh, Rajendra, et al. "Sustainable Rural Telehealth Innovation: A Public Health Case Study." Health Services Research, vol. 45, no. 4, 2010, pp. 985–1004., doi:10.1111/j.1475-6773.2010.01116.x.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with Information Security Policies: An Empirical Investigation. Computer, 43(2), 64–71. doi: 10.1109/mc.2010.35

Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. MIS Quarterly, 34(3), 487–502. doi: 10.2307/25750688

Smith, Wendy K. "Dynamic Decision Making: A Model of Senior Leaders Managing Strategic Paradoxes." *Academy of Management Journal*, vol. 57, no. 6, 2014, pp. 1592–1623., doi:10.5465/amj.2011.0932.

Smith, J. A., Flowers, P., & Larkin, M. H. (2013). Interpretative phenomenological analysis: theory, method and research. Los Angeles: Sage.

Smith, K. K., & Berg, D. N. (1997). Paradoxes of group life understanding conflict, paralysis, and movement in group dynamics. San Francisco, CA: Jossey-Bass.

Smith, W. K., & Lewis, M. W. (2011). Toward A Theory Of Paradox: A Dynamic Equilibrium Model Of Organizing. Academy of Management Review, 36(2), 381–403. doi: 10.5465/amr.2011.59330958

Straub, D. W. (1990). Effective IS Security: An Empirical Study. Information Systems Research, 1(3), 255–276. doi: 10.1287/isre.1.3.255

Sykes, G. M., & Matza, D. (1957). Techniques of Neutralization: A Theory of Delinquency. American Sociological Review, 22(6), 664–670. doi: 10.2307/2089195

Tilson, David, et al. "Change and Control Paradoxes in Mobile Infrastructure Innovation: The Android and IOS Mobile Operating Systems Cases." 2012 45th Hawaii International Conference on System Sciences, 2012, doi:10.1109/hicss.2012.149.

Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. Computers & Security, 45, 42–57. doi: 10.1016/j.cose.2014.05.003

Tracy, Joseph, et al. "Critical Steps to Scaling Telehealth for National Reform." Telemedicine and e-Health, vol. 14, no. 9, 2008, pp. 990–994., doi:10.1089/tmj.2008.0125.

Vagle, M. D. (2018). Crafting phenomenological research (2nd ed.). New York, NY: Routledge.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. Information & Management, 49(3-4), 190–198. doi: 10.1016/j.im.2012.04.002

Van de Ven, A. H. (2013). Engaged scholarship: a guide for organizational and social research. Oxford: Oxford University Press.

van Manen, M. (2014). Phenomenology of practice: meaning-giving methods in phenomenological research and writing. Walnut Creek, CA: Left Coast Press.

Vince, R., & Broussine, M. (1996). Paradox, Defense and Attachment: Accessing and Working with Emotions and Relations Underlying Organizational Change. Organization Studies, 17(1), 1–21. doi: 10.1177/017084069601700101

Walsham, G. (1995). Interpretive case studies in IS research: nature and method. European Journal of Information Systems, 4(2), 74–81. doi: 10.1057/ejis.1995.9

Westen, P., & Mangiafico, J. (2004). The Criminal Defense of Duress: A Justification, Not an Excuse——And Why It Matters. Buffalo Criminal Law Review, 6(2), 833-950. doi:10.1525/nclr.2003.6.2.833

Wiant, T. L. (2005). Information security policys impact on reporting security incidents. Computers & Security, 24(6), 448–459. doi: 10.1016/j.cose.2005.03.008

Wimelius, H., Mathiassen, L., Holmström, J., Keil, M. (2020). A paradoxical perspective on technology renewal in digital transformation. Accepted for publication in Information Systems Journal 2020

Workman, M., & Gathegi, J. (2006). Punishment and ethics deterrents: A study of insider security contravention. Journal of the American Society for Information Science and Technology, 58(2), 212–222. doi: 10.1002/asi.20474

Yin, R. K. (2018). Case study research and applications: design and methods (6th ed.). Los Angeles: Sage.

APPENDICES

Table 2: Paradoxical Perspective in Information Security Reporting

Concepts	Definitions and Claims	References
Information security professionals as potential insider threats	Information security professionals must deal with many of the same competing tensions that lead to insider deviant behavior. In addressing these tensions, the perceptions generated induce the motivations and behaviors that may evolve into insider threats to an organization.	Crossler et al., 2013 Elifoglu et al., 2018
Paradoxical tensions	Information security reporting involves inherent tensions between complying with organizational security policy requirements and competing demands such as opposing management directives or orders to act in a deviant manner. Information security professionals may be coerced or threatened into committing deviant acts, forcing them to encounter the salient tension of complying or violating security policy.	Lewis, 2000 Putnam at al., 2016 Lewis and Smith, 2014
Individual responses	When information security professionals experience paradoxical tensions, they may engage in choosing one tension over the other (splitting), move to include a third party such as human resources (projecting), mentally repress their role in the act (regression), or physically remove themselves from the tension by seeking other employment (withdrawal).	Lewis, 2000 Tracy, 2000
Insider deviant behavior under duress	An information security professional will act in a deviant manner when under duress, such as when an external actor uses force, fear, or coercion to force compliance. While under duress, the security professionals' perceived ability to act against this duress will be gauged by their perceived level of fault responsibility and time urgency.	Park et al., 2008

Duress	An affirmative defense for information security professionals who engage in behavior that would be considered deviant but are coerced to do so by the use of force or the threat of force against themselves or against another; furthermore, these security professionals, being of reasonable firmness in their situation, would be unable to resist this coercion.	Brink, 2018 Fletcher, 1998 Model Penal Code, Sec. 2.09(1)

About the Author

Robin L. Moore is a veteran information security professional with over a decade of IT and security know-how and experience covering physical security, application security, security audit, and vendor management. Robin also serves as a board member on the Georgia State University Alumni Association Board of Directors and as a board member on the Metro Atlanta ISSA Board of Directors. Robin, who holds a Master of Science in Information Systems (MSIS) degree, is a Certified Information Systems Security Professional (CISSP) and a Certified Ethical Hacker (CEH). His research is focused on the phenomenon of human behavior in the field of information systems security.